Bosna i Hercegovina
Federacija Bosne i Hercegovine
AGENCIJA ZA DRŽAVNU SLUŽBU

Danijela Radonić, MA

PRIMJENA ZAKONA O ZAŠTITI LIČNIH PODATAKA BIH



22/10/2025 | 8:30 -10:30

CILJEVI EDUKACIJE

- Upoznavanje sa odredbama novog Zakona o zaštiti ličnih podataka,
- Predstavljanje ključnih obaveza kontrolora u javnom sektoru,
- Sagledavanje obaveza u pogledu donošenja akata

Teme

M1 Novi Zakon o zaštiti ličnih podataka

- Područje primjene ZZLP
- Lični podatak, nosilac ličnih podataka, kontrolor, obrađivač
- Javni organ, nadležni organ, primalac, treća strana
- Principi obrade
- Saglasnost
- Obrada posebnih kategorija ličnih podataka
- Posebni slučajevi obrade
- Video-nadzor

M2 Obaveze kontrolora u javnom sektoru

- Tehničke i organizacione mjere
- Tehnička i integrisana zaštita podataka – privacy by design i privacy by default
- Pseudonimizacija, enkripcija, smanjenje količine podataka
- Evidencija o obradi ličnih podataka
- Postupanje u slučaju povrede ličnog podataka
- Službenik za zaštitu ličnih podataka
- Prenos ličnog podatka u drugu državu ili međunarodnu organizaciju
- **Akti kontrolora za primjenu novog Zakona o zaštiti ličnih podataka**

UVOD

ESLJP u Strazburu tretira zaštitu ličnosti u vezi sa obradom podataka kao dio prava na privatnost što je garantovano članom 8. EKLJP.

Pravo na zaštitu ličnih podataka nije apsolutno pravo; moramo ga posmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim osnovnim pravima u skladu s načelom proporcionalnosti.

PRAVNI OKVIR ZAŠTITE LP U BIH

Pravni okvir – dokumenti u Bosni i Hercegovini

•Ustav Bosne i Hercegovine / entiteta

•Lex specialis

•Sporazum o stabilizaciji i pridruživanju između evropskih zajednica i njihovih država članica i Bosne i Hercegovine **(krajnji rok 01.06.2021.)**

Međunarodni dokumenti

•Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (1950)

•Povelja Evropske unije o osnovnim pravima

•Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46 EZ - Opšta uredba o zaštiti ličnih podataka – GDPR

•Direktiva (EU) 2016/680 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi sa obradom ličnih podataka koju vrše nadležna tijela radi sprečavanja, istrage, otkrivanja krivičnih djela ili gonjenja učinilaca krivičnih djela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka te o stavljanju van snage Okvirne odluke Savjeta 2008/977/PUP

NOVI ZZLP

- Konačno je usvojen krajem januara 2025. godine
- Objava Službeni glasnik BIH, broj 12/2025
- stupio je na snagu 8.3.2025. godine, sa odloženim rokom primjene od 210 dana.

Početak primjene Zakona je **4. oktobar 2025. godine**.

Novi Zakon, pored pravila zaštite ličnih podataka, obuhvata i pravila iz tzv. Policijske direktive.

Područje primjene

Glavna oblast primjene

ZZLP se primjenjuje na obradu ličnog podatka koja se u potpunosti obavlja automatizovano te na neautomatizovanu obradu ličnog podatka koji čini dio zbirke ličnih podataka ili je namijenjen da bude dio zbirke ličnih podataka.

ZZLP se **ne primjenjuje** na obradu ličnog podatka koju obavlja fizičko lice isključivo u svrhu ličnih aktivnosti ili aktivnosti domaćinstva.

Na obradu ličnog podatka od nadležnog organa u svrhu zaštite fizičkih lica u vezi s obradom ličnih podataka u svrhu sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinilaca krivičnih djela, izvršenja krivičnih sankcija, uključujući i zaštitu od prijetnji javnoj bezbjednosti i njihovo sprečavanje, ne primjenjuje se DIO DRUGI ZZLP.

Postupanje ovih organa u ove svrhe detaljno je uređeno DIJELOM TREĆIM ZZLP – čl. Od 60. do 95. koji sadrže posebne odredbe.

Tzv. Policijska direktiva (2016/680) ugrađena je u ZZLP (čl. 60-95) zbog čega je obrada koju vrše organi za sprovođenje zakona u određenoj mjeri razlikuje od obrade koju vrše drugi kontrolori:

- Nema volje nosioca podatka da svoje podatke sam ustupi.
- Ne zahtijeva se transparentnost obrade podataka.
- Ublažena je obaveza svođenja količine podataka na minimum.
- Prava lica na koja se podaci odnose mogu se bitno ograničiti.

Teritorijalno područje primjene

ZZLP se primjenjuje na obradu ličnog podatka koju obavlja kontrolor podataka ili obrađivač koji ima sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, nezavisno od toga obavlja li se obrada u Bosni i Hercegovini ili ne.

ZZLP se primjenjuje na obradu ličnog podatka nosioca podataka u Bosni i Hercegovini koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, ako je aktivnost obrade povezana sa:

a)nuđenjem robe ili usluga tim nosiocima podataka u Bosni i Hercegovini, nezavisno od toga da li nosilac podataka treba da izvrši plaćanje, ili

b) praćenjem ponašanja nosilaca podataka, uz uslov da se njihovo ponašanje odvija unutar Bosne i Hercegovine.

ZZLP se primjenjuje na obradu ličnog podatka koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan u Bosni i Hercegovini već u mjestu gdje se pravo Bosne i Hercegovine primjenjuje na osnovu međunarodnog prava.

Na obradu ličnog podatka od nadležnog organa u svrhu zaštite fizičkog lica u vezi s obradom ličnog podatka u svrhu sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinilaca krivičnih djela, izvršenja krivičnih sankcija, uključujući i zaštitu od prijetnji javnoj bezbjednosti i njihovo sprečavanje, ne primjenjuje se ovaj član.

Definicije

Čl. 4. ZZLP – postojeće + nove

Ukupno je 26 definicija sadržano u članu 4. ZZLP.

Lični podatak je određen uopštenom definicijom, ali i pomoćnom.

1. Lični podatak je svaki podatak koja se odnosi na fizičko lice čiji je identitet utvrđen ili se može utvrditi.

Ovakva definicija potiče iz Konvencije o zaštiti lica u odnosu na automatsku obradu podataka Savjeta Evrope, broj 108/1981.

2. Nosilac podatka je FL čiji se identitet utvrđen ili se može utvrditi posredeno ili neposredno, posebno uz pomoć identifikatora:

- ime,
- identifikacioni broj,
- podaci o lokaciji,
- mrežni identifikator ili
- uz pomoć jednog ili više faktora karakterističnih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Novinu u određenju ličnog podatka predstavljaju:

-**ime –** podrazumijeva ime i prezime na način kako su isti određeni propisima o ličnom odnosno porodičnom imenu. Kod ovog podatka treba imati u vidu i javni interes koji načelno podrazumijeva slobodu pristupa informacijama kod pitanja koja se odnose na javna sredstva odnosno raspolaganje tim sredstvima. Kada se radi o raspolaganju javnim sredstvima, ime i prezime fizičke osobe ne smatra se zaštićenim ličnim podatkom.

- **identifikacioni broj** je širi pojam od jedinstvenog matičnog broja koji je do sada važio kao identifikator ličnog podatka. On podrazumijeva bilo koji identifikacioni broj: identifikacioni broj radnika, identifikacioni broj člana udruženja, matični broj osiguranika penzijskog sistema, lični/osobni identifikacioni broj (PU FBIH), broj pasoša, broj lične karte, broj zdravstvene iskaznice, i sl.

-**podaci o lokaciji** – imaju dvostruki karakter:

-1. odnose se na boravak nekog lica na određenom području (npr. boravak u nekom gradu, radno mjesto, mjesto stanovanja ili uobičajenog boravka), dok

-2. se odnose na mogućnost izrade profila kretanja nekog lica i druge forme profilisanja, koje omogućavaju identifikaciju lica uz pomoć njenog kretanja, analize ili prognoze njenog kretanja. To se može postići i lokacijom uređaja npr. pametnog telefona ili GPS.

- **mrežni identifikator – IP adresa** Internet priključka, identifikator mobilnog telefona pod određenim okolnostima smatraju se ličnim podatkom. Navedeni identifikatori, sami po sebi ne predstavljaju lični podatak, ali kombinacijom dva ili više navedenih identifikatora moguće je direktno ili indirektno utvrditi identitet pojedinca, pa time u kombinaciji postaju lični podatak. To je vidljivo iz presude Evropskog suda pravde u predmetu 582/14 – Patrick Breye protiv Njemačke u kojoj je iskazan stav da IP adresa pod određenim okolnostima predstavlja lični podatak.

- **faktor svojstven genetskom identititetu lica** – koji proizilazi iz razvoja genetike (engl. genetics), biološke nauke koja istražuje nasljeđivanje i raznolikost genetičke informacije, odnosno kako se prenose svojstva roditelja na potomstvo, zbog čega nasljedna svojstva kod jedinki istih roditelja variraju, koji faktori određuju ta svojstva, na koji se način svojstva mijenjaju i stiču nova.

3. Obrada je, kao i do sada, svaki postupak ili skup postupaka koji se obavlja na ličnim podacima ili na skupovima ličnih podataka, automatiziranim ili neautomatiziranim sredstvima, kao što su prikupljanje, evidentiranje, organizacija, strukturiranje, čuvanje, prilagođavanje ili izmjena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombinovanje, ograničenje, brisanje ili uništavanje. Ukratko,obrada ličnih podataka predstavlja svaku radnju kojom se upravlja ličnim podacima jednog ili više lica.

4. Sa obradom je povezano **ograničenje obrade** koje se definiše kao obilježavanje čuvanog ličnog podatka s ciljem ograničenja njegove obrade u budućnosti.

5. Izrada profila (profilisanje) je svaki oblik automatske obrade ličnog podatka koji se sastoji od korištenja ličnog podatka za procjenu određenih ličnih aspekata u vezi s fizičkim licem, posebno za analizu ili predviđanje aspekata u vezi s radnim rezultatom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog fizičkog lica. Iz ove definicije može se zaključiti da se radi o jednoj posebnoj analizi i procjeni ličnih podataka.

6. Pseudonimizacija je obrada ličnog podatka tako da se lični podatak više ne može pripisati određenom nosiocu podataka bez korištenja dodatnih informacija, uz uslov da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacionim mjerama kako bi se osiguralo da se lični podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi. To je jedna od tehničko-organizacionih mjera koja ima za cilj da se podaci o pseudonimima koriste kao posredno utvrdivi lični podaci.

7. Zbirka ličnih podataka je svaki strukturirani skup ličnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to jesu li centralizovani, decentralizovani ili rasprostranjeni na funkcionalnoj ili geografskoj osnovi.

8. Kontrolor podataka je fizičko ili pravno lice, javni organ ili nadležni organ koji samostalno ili s drugim određuje svrhe i sredstva obrade ličnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriteriji za njegovo imenovanje propisuju se zakonom. Bitno je ukazati da je ova definicija postavljena nešto drugačije od postojeće, jer je do sada bilo propisano da kontrolor obrađuje i utvrđuje svrhu i način obrade ličnih podataka na osnovu zakona ili propisa.

Kontrolor donosi odluku kojom utvrđuje zašto se i kako podaci obrađuju.

9. Javni organ je svaki zakonodavni, izvršni i sudski organ na svim nivoima vlasti u BiH. To podrazmijeva ove organe u entitetima, kantonima i jedinicama lokalne samouprave.

10. Nadležni organ je organ koji je nadležan za sprečavanje, istragu i otkrivanje krivičnih djela, gonjenje učinilaca krivičnih djela ili izvršenje krivičnih sankcija, uključujući i zaštitu i sprečavanje prijetnji javnoj sigurnosti, kao i pravna lica ako su zakonom ovlaštena za obavljanje tih poslova, kao posebna kategorija kontrolora podataka. Za ovu vrstu kontrolora predviđena su posebna pravila sadržana u djelu trećem novog ZZLP.

11. Obrađivač je fizičko ili pravno lice, javni organ koji obrađuje lične podatke u ime kontrolora podataka. Iako ova definicija dugo egzistira sada sve više dobija na značaju. Mnoge usluge se ustupaju koopernatima (tzv. outsourcing), ali oni su samo opcija. On obradu podataka vrši na osnovu ugovora u pisanoj formi koji zaključi sa kontrolorom.

12. Primalac je, kao i do sada, fizičko ili pravno lice, javni organ kome se otkrivaju lični podaci, nezavisno od toga da li je u pitanju treća strana. No kako je u novi ZZLP ugrađena i tzv. Policijska direktiva ova definicija je sada proširena na način da se javni organi koji mogu primiti lične podatke u okviru određene istrage u skladu sa zakonom ne smatraju primaocima, ali obrada tih podataka mora biti u skladu s važećim pravilima o zaštiti podataka prema svrhama obrade.

13. Treća strana znači fizičko ili pravno lice, javni organ, Agencija za zaštitu ličnih podataka ili drugo tijelo koji nije nosilac podataka, kontrolor podataka, obrađivač ni lica koja su ovlaštena za obradu ličnih podataka pod neposrednom nadležnošću kontrolora podataka ili obrađivača.

14. Saglasnost nosioca podataka je svako dobrovoljno, posebno, informisano i nedvosmisleno izražavanje volje nosioca podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu ličnih podataka koji se na njega odnose. Na isti način kako se daje saglasnost ona može biti i povučena, s tim da eventualno povlačenje saglasnosti ne utiče na zakonitost obrade podataka na osnovu saglasnosti prije njenog povlačenja.

15. Povreda ličnog podatka (eng. data breach) je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa ličnim podacima koji su preneseni, čuvani ili na drugi način obrađivani. Uništavanje ličnih podataka podrazumijeva da podaci više ne postoje ili ne postoje u obliku koji je od bilo kakve koristi kontroloru. Takvi podaci su izmijenjeni, zloupotrebljeni ili nisu više kompletni. Gubitak ličnih podataka podrazumijeva da podaci i dalje postoje, ali je kontrolor izgubio kontrolu ili pristup nad njima, ili podatke više ne posjeduje. Neovlašteno otkrivanje ili pristup podacima može obuhvatati otkrivanje ličnih podataka primaocima ili pristup podacima licima koja nisu ovlašćena da primaju ili pristupe podacima ili bilo koji drugi oblik obrade koji je u suprotnosti sa ZZLP.

16. Genetski podatak je lični podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičkog lica koja daju jedinstvene informacije o fiziologiji ili zdravlju tog fizičkog lica i koji su dobijeni posebnom analizom biološkog uzorka tog fizičkog lica. Biološka analiza podrazumijeva analizu hromozoma, dezoksiribonukleinska kiselina (DNK), ribonukleinska kiselina (RNK) i sl. Ranije ovaj pojam nije bio zakonom definisan, tako da ovo definisanje predstavlja pomak u razumijvanju a time i zaštiti ličnog podatka.

17. Biometrijski podatak je lični podatak dobijen posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičkog lica koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica, kao što su fotografije lica ili daktiloskopski podaci.

Radi pojašnjenja ukazujem da se u biometrijske podatke ubrajaju i:

- otisak prsta/otisci prstiju,
- hod,
- potpis,
- glas,
- dinamika kucanja,
- mrežnica oka i dr.

No to nije dovoljno za utvrđivanje identiteta, te je potrebno i posjedovanje biometrijskog šablona, algoritma i šablona u običnom formatu.

18. Podatak koji se odnosi na zdravlje je lični podatak u vezi s fizičkim ili mentalnim zdravljem fizičkog lica, uključujući pružanje zdravstvenih usluga, koji daje informacije o njegovom zdravstvenom stanju. To podrazumijeva informacije o bolesti, invaliditetu, rizicima bolesti, istoriji bolesti, kliničkom liječenju, fiziološkom ili biomedicinskom stanju. Šifra bolesti na potvrdi o trajanju privremene nesposobnosti za rad je najčešći primjer zdravstvenog podatka koji se dostavlja poslodavcu.

19. Predstavnik je fizičko ili pravno lice s prebivalištem ili boravištem, odnosno sjedištem ili poslovnim nastanom u Bosni i Hercegovini koje je kontrolor podataka ili obrađivač pisanim putem imenovao u skladu s članom 29. novog ZZLP.

20. Privredni subjekat je fizičko ili pravno lice koje obavlja privrednu djelatnost, bez obzira na pravni oblik te djelatnosti.

21. Grupa privrednih subjekata je privredni subjekt koji ostvaruje kontrolu i privredni subjekti koji su pod njegovom kontrolom.

22. Obavezujuće poslovno pravilo su politike zaštite ličnih podataka kojih se kontrolor podataka i obrađivač sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini pridržava prilikom prenosa ili skupova prenosa ličnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih država u okviru grupe privrednih subjekata ili grupe privrednih subjekata koji se bave zajedničkom privrednom djelatnošću.

23. Usluga informacionog društva jeste svaka usluga koja se obično pruža uz naknadu, na daljinu, elektronskim sredstvima te na lični zahtjev primaoca usluga, gdje:

1) „na daljinu" znači da se usluga pruža a da pri tome strane nisu istovremeno prisutne;

2) „elektronskim sredstvima" znači da se usluga na početku šalje i prima na odredištu pomoću elektronske opreme za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radiovezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima;

3) „na lični zahtjev primaoca usluga" znači da se usluga pruža prenosom podataka na lični zahtjev.

24. Međunarodna organizacija je organizacija sa svojim organima uređena međunarodnim javnim pravom ili bilo koji drugi organ koji su sporazumom ili na osnovu sporazuma osnovale dvije zemlje ili više zemalja.

25. Poslovni nastan je djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana.

26. Video-nadzor je informacijsko-komunikacijski sistem koji ima mogućnost prikupljanja i daljnje obrade ličnih podataka, koji obuhvata stvaranje snimka koji čini ili je namijenjen da čini dio sistema skadištenja.

Principi obrade

Pored zakonitosti obrade (čl. 8. ZZLP) principi obrade su od suštinskog značaja za usaglašenost kontrolora i obrađivača sa ZZLP.

Svaka aktivnost obrade treba da bude u skladu sa principima iz člana 7. ZZLP.

Postoji 8 načela i 1 supra-načelo (7/2) – načelo nad načelima!

Imaju višestruk značaj.

1. **zakonitost –** postojanje odgovarajućeg pravnog osnova
2. **pravičnost -** imati u vidu interese FL i ponašati se pošteno u konkretnim okolnostima
3. **transparentnost** – pravo FL na informisanje od početka....
4. **ograničenje svrhe (vezanost za svrhu)** – podaci su prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, u skladu sa članom 56. stav (1) ZZLP ne smatra se neusklađenom sa prvobitnim svrhama.

5. **smanjenje obima podataka –** podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhe u koje se obrađuju.

6. **tačnost –** podaci moraju biti tačni i prema potrebi ažurirani; treba preduzeti sve razumne mjere kako bi se obezbijedilo da lični podaci, koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni

7. **ograničenje čuvanja -** podaci moraju biti čuvani u formi koja omogućava identifikaciju nosioca podataka i to ne duže nego što je potrebno u svrhe u koje se lični podaci obrađuju.

Lični podaci se mogu čuvati na duži period ako će se lični podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe, što podliježe provođenju primjerenih tehničkih i organizacionih mjera propisanih novim Zakonom radi zaštite prava i sloboda vlasnika podataka.

8. **cjelovitost i povjerljivost –** podaci moraju biti obrađivani tako da se osigura odgovarajuća bezbjednost ličnih podataka, uključujući i zaštitu od neovlašćene ili nezakonite obrade i slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera

SUPRA-NAČELO:

Princip pouzdanosti

kontrolor podataka:

1) odgovoran je za usklađenost obrade ličnog podatka sa stavom (1) člana 7. i
2) mora biti u mogućnosti dokazati tu usklađenost.

U GDPR označeno kao n. pouzdanosti, mada se u nekim sistemima ovo načelo ozačava kao n. društvene odgovornosti.

Dokazivanje:

1)Obavezujuća poslovna pravila

2)Sertifikacija

ZAKONITOST OBRADE

Zakonitost obrade podrazumijeva pravo kontrolora da vrši obradu samo ako je ona bazirana na jednom od 6 raspoloživih pravnih osnova.

U suprotnom, obrada je nezakonita.

Osnovi:

1. saglasnost za obradu svojih ličnih podataka u jednu ili više posebnih svrha;

2)ako je obrada neophodna radi izvršenja ugovora u kojem je nosilac podataka ugovorna strana ili radi preduzimanja radnji na zahtjev nosioca podataka prije zaključenja ugovora;

3) ako je obrada neophodna radi poštovanja pravnih obaveza kontrolora podataka;

4) ako je obrada neophodna radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica;

5) ako je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka;

6) ako je obrada neophodna zbog legitimnih interesa kontrolora podataka ili treće strane, osim kada nad tim interesima pretežu interesi ili osnovna prava i slobode nosioca podataka, a koji zahtijevaju zaštitu ličnih podataka, posebno ako je nosilac podataka dijete. Ova tačka se ne primjenjuje na obradu koju rade javni organi pri obavljanju svojih poslova.

Saglasnost

nosioca podataka je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje nosioca podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu ličnih podataka koji se na njega odnose.

Primjer: slanje fotografije za web stranicu poslodavca

Saglasnost nosioca ličnog podatka

Saglasnost:

- ✓ pisana forma,
- ✓potpis nosioca podataka, te
- ✓tačna naznaka podataka u vezi s kojima se saglasnost za obradu ličnih podataka daje,
- ✓ime kontrolora, svrhu i vremenski period na koji se saglasnost daje.

Kada je obrada zasnovana na saglasnosti, kontrolor podataka mora dokazati da je nosilac podataka dao saglasnost za obradu svojih ličnih podataka.

Ako nosilac podataka daje saglasnost u pisanoj izjavi koja se odnosi i na druga pitanja, zahtjev za saglasnost mora biti predstavljen tako da se jasno razlikuje od drugih pitanja, u razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika. Dio saglasnosti koji predstavlja kršenje ovog zakona se ne primjenjuje.

Nosilac podataka ima pravo u bilo kojem trenutku povući svoju saglasnost.

Povlačenje saglasnosti ne utiče na zakonitost obrade podataka na osnovu saglasnosti prije njenog povlačenja.

Prije davanja saglasnosti nosilac podataka se o tome obavještava.

Povlačenje saglasnosti mora biti jednako jednostavno kao i njeno davanje.

Kada se procjenjuje da li je saglasnost data dobrovoljno, u najvećoj mogućoj mjeri se uzima u obzir da li je, između ostalog, izvršenje ugovora, uključujući i pružanje usluge, uslovljeno saglasnošću za obradu ličnih podataka koja nije neophodna za izvršenje tog ugovora.

Saglasnost djeteta u vezi sa uslugama inf. društva

Kada se primjenjuje saglasnost u pogledu neposrednog nuđenja usluga informacionog društva djetetu, obrada ličnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina. Ako je dijete mlađe od 16 godina, takva obrada je zakonita samo ako i u mjeri u kojoj je saglasnost dao ili odobrio roditelj, usvojilac, staratelj djeteta ili drugi zastupnik djeteta.

Kontrolor podataka mora uložiti razumne napore prilikom provjere da li je saglasnost u tim slučajevima dao ili odobrio roditelj, usvojilac, odnosno staratelj djeteta, uzimajući u obzir dostupnu tehnologiju.

Stav (1) ovog člana ne utiče na opšta pravila obligacionog prava koja se tiču važenja, zaključenja ili učinka ugovora u vezi s djetetom.

Obrada posebnih kategorija ličnih podataka

Posebna kategorija su podaci koji otkrivaju:

- rasno ili etničko porijeklo,
- politička mišljenja,
- vjerska ili filozofska uvjerenja,
- pripadnost sindikatu,
- obrada genetskih podataka,
- biometrijskih podataka u svrhu jedinstvene identifikacije lica,
- podataka o zdravlju,
- podataka o spolnom životu,
- seksualnoj orijentaciji lica.

ZABRANJENA JE

Dozovoljena je ako je ispunjen jedan od sljedećih uslova:

- **ako je nosilac podataka dao izričitu saglasnost za obradu tih ličnih podataka za jednu ili više konkretnih svrha, osim kada je posebnim zakonom propisano da se obrada tih podataka ne može obavljati na osnovu saglasnosti;**
- obrada je neophodna radi:

❖ u oblasti radnog prava i prava socijalnog osiguranja i socijalne zaštite,

❖ zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica ako nosilac podataka fizički ili pravno ne može dati saglasnost;

❖ Obrade koja se obavlja u okviru legitimnih aktivnosti, uz odgovarajuće zaštitne mjere, fondacije, udruženja ili bilo koje druge neprofitne organizacije s političkim, filozofskim, vjerskim ili sindikalnim ciljem i to uz uslov da se obrada odnosi isključivo na članove ili bivše članove te organizacije ili na fizička lica koja imaju redovan kontakt s njom, a u vezi s njenim svrhama i da se lični podaci ne otkrivaju van te organizacije bez saglasnosti nosioca podataka;

- ako se obrada odnosi na lične podatke za koje je očito da ih je objavio nosilac podataka;
- ako je obrada neophodna za uspostavljanje, ostvarivanje ili odbranu pravnih zahtjeva ili kad sudovi postupaju u sudskom svojstvu;
- ako je obrada neophodna za potrebe značajnog javnog interesa, na osnovu zakona koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu ličnih podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka;
- ako je obrada neophodna za potrebe preventivne medicine ili medicine rada zbog procjene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili socijalne zaštite ili tretmana ili upravljanja sistemima i uslugama zdravstvene ili socijalne zaštite na osnovu posebnog zakona ili u skladu s ugovorom sa zdravstvenim radnikom i uz uslove i mjere zaštite iz stava (3) člana 11.;

- ako je obrada neophodna iz razloga javnog interesa u oblasti javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih prijetnji za zdravlje ili osiguranje visokih standarda kvaliteta i sigurnosti zdravstvene zaštite i lijekova i medicinskih sredstava, na osnovu posebnog zakona kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda nosioca podataka, a posebno čuvanje profesionalne tajne;
- ako je obrada neophodna za potrebe arhiviranja u javnom interesu, potrebe naučnog ili historijskog istraživanja ili statističke potrebe u skladu s članom 56. stav (1) ovog zakona, a na osnovu posebnog zakona, koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka.

Posebni slučajevi obrade

1. Obrada LP i sloboda izražavanja i informisanja:

- obrada u novinarske svrhe;
- u svrhe akademskog, umjetničkog ili književnog izražavanja

POSEBNIM ZAKONOM mogu se utvrditi odstupanja od Glava I, II, III, IV V ovog dijela i dijela četvrtog ZZLP

Sloboda izražavanja i informisanja načelno ima prednost!

2. Obrada LP i javni pristup službenim dokumentima

Javni organ može u javnom interesu otkriti LP iz službenih dokumenata

ZZLP se primjenjuje prilikom primjene ZSPI.

(3) Institucije BiH, odnosno svaka fizička ili pravna osoba na koju se odnose odredbe ovog zakona dužna je dosljedno postupiti po odredbama Zakona o zaštiti osobnih podataka („Službeni glasnik BiH“, br. 49/06, 76/11 i 89/11).

Prilikom rješavanja zahtjeva za pristup informacijama, odnosno zahtjeva za davanje podataka, kontrolori u skladu sa definicijama mjerodavnih propisa moraju razgraničiti šta je

Informacija „svaki materijal kojim se prenose činjenice, mišljenja, podaci ili bilo koji drugi sadržaj, uključujući svaku presliku ili njen dio, bez obzira na oblik, karakteristike, vrijeme kada je sačinjena i kako je klasificirana". - čl. 3. st.1. ZSPI - npr., imena radnika _____ BIH, funkcije koje obavljaju, datum zaključenja ugovora o djelu/radu na određeno vrijeme/radu na neodređeno vrijeme, važnosti ugovora smatraju se informacijama u smislu ZSPI.

Lični podatak „bilo koja informacija koja se odnosi na fizičku osobu na osnovu koje je utvrđen ili se može utvrditi identitet osobe”, a “nositelj podataka” je: „fizička osoba čiji se identitet može ustanoviti ili identificirati, neposredno ili posredno, naročito na osnovu jedinstvenog matičnog broja te jednog ili više čimbenika karakterističnih za fizički, fiziološki, mentalni, privredni, kulturni ili socijalni identitet te osobe”.

Čl. 3. st. 1. ZZLP - npr. lični podaci radnika BiH bi bili oni podaci koji se odnose na JMB, iznos plate, broj protokola pod kojim se ugovor o djelu/radu vodi u instituciji sa kojom je ugovor zaključen, broj članova kućnog domaćinstva, imena članova kućnog domaćinstva, adresa stanovanja, broj telefona i slično.

3. Obrada JMBG

U skladu sa posebnim zakonom

Ako je to propisano zakonom, organi i druge pravne osobe koje na temelju zakona vode evidencije o građanima i na temelju tih službenih evidencija izdaju javne isprave dužne su da koriste JMB.

Samo ako je to zakonom izrijekom propisano, JMB se upisuje u osobnu iskaznicu, izvod iz MKR/V/U, radnu knjižicu, zdravstvenu iskaznicu, putnu ispravu, vozačku dozvolu, oružni list, evidenciju o državljanstvu, kao i druge evidencije i javne isprave građana.

Prilikom promjene prebivališta, JMB se upisuje u potvrdu o prijavi odnosno odjavi prebivališta.

JMB upisan u LK služi kao temelj za upisivanje JMB u sve druge javne isprave i evidencije.

ZAKON
O JMB (SGBiH br. 32/2001, 63/08, 103/11, 87/13, 84/15)

propisuje se određivanje, dodjeljivanje, upisivanje, korištenje, evidencija, struktura, poništenje i zamjena JMB državljana BIH i stranih državljana u BIH.

Postupak obrade podataka vrši se u skladu sa ZZLP i Zakonom o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka BIH (SGBiH broj 56/08).

Postoji cca 25 podzakonskih akata.

PROMJENA POLA - JMBG

Promjena imena – Zakon o matičnim knjigama čl. 12 – MKR, Zak. o ličnom imenu

Promjena JMB DDMMGGGRRBBBK

Dio matičnog broja osobe koji se odnosi na dan rođenja (I. grupa), mjesec rođenja (II. grupa), godinu rođenja (III. grupa) i spol (V. grupa) određuje nadležni organ na temelju podataka o toj osobi iz izvoda iz matične knjige rođenih.

Organ koji donosi rješenje o ispravci upisanog dana, mjeseca i godine rođenja kao i organ koji donosi rješenje o upisu promjene spola i potpunog usvojenja dužan je u roku od 30 dana od pravosnažnosti rješenja dostaviti jedan primjerak rješenja nadležnom organu.

Nakon što primi to rješenje nadležni organ u roku od 15 dana poništava JMB i izdaje novi. Nadležni organ obavještava lice koje je u pitanju i organ koji donosi rješenje kako bi ih izvijestio o novom JMB.

OBRADA PODATAKA U KONTEKSTU ZAPOŠLJAVANJA

Posebnim zakonom ili kolektivnim ugovorom preciziraju se pravila s ciljem obezbjeđivanja zaštite prava i sloboda u vezi s obradom ličnih podataka u kontekstu zaposlenja, posebno za potrebe:

- zapošljavanja,
- izvršenja ugovora o radu, uključujući i izvršavanje obaveza propisanih zakonom ili kolektivnim ugovorima,
- za potrebe upravljanja, planiranja i organizacije rada, jednakosti i različitosti na radnom mjestu,
- zdravstva i bezbjednosti na radu,
- zaštite imovine poslodavca ili klijenta i
- za potrebe individualnog ili kolektivnog ostvarivanja i uživanja prava i pogodnosti iz radnog odnosa, kao i
- za potrebe prestanka radnog odnosa.

ZOR



Čl. 102. ZOR

✓Radnik ima pravo uvida u sve dokumente, kao i pravo da zahtijeva brisanje podataka koji nisu od neposrednog značaja za poslove koje obavlja, kao i ispravljanje netačnih podataka,

✓Lični podaci koji se odnose na radnika ne mogu da budu dostupni trećem licu (izuzetak – utvr. zakonom ili ako je to potrebno radi dokazivanja prava i obaveza iz radnog odnosa ili u vezi sa radom),

✓ovlašćeno lice zaposleno kod poslodavca u skladu sa propisom koji uređuje zaštitu ličnih podatka.

čl. 30. ZOR FBIH / čl. 22 ZOR BD

Lični podaci radnika ne mogu se prikupljati, obrađivati, koristiti ili dostavljati trećim licima, osim ako je to određeno zakonom ili ako je to potrebno radi ostvarivanja prava i obaveza iz radnog odnosa.

KONKURS

Kandidat je dužan da prilikom zasnivanja radnog odnosa poslodavcu dostavi isprave i druge dokaze o ispunjenosti uslova za rad na poslovima za koje zasniva radni odnos (NE podatke o porodičnom, odnosno bračnom statusu i planiranju porodice, odnosno dostavljanje isprava i drugih dokaza koji nisu od neposrednog značaja za obavljanje poslova za koje se zasniva radni odnos, niti da uslovljava zasnivanje radnog odnosa testom trudnoće, osim ako je riječ o poslovima kod kojih postoji znatan rizik za zdravlje žene i djeteta utvrđen od nadležnog zdravstvenog organa, odnosno aktom o procjeni rizika).

Javni konkurs – Uredba o postupku prijema u radni odnos u javnom sektoru u FBIH (SNFBiH 13/2019, 9/21, 53/21) i Uredba o postupku prijema u radni odnos …. (SN KS 19/21 i 10/22)

Pravo uvida u rezultate procedure prijema u radni odnos član 13. Uredbe FBIH

Po prijemu obavještenja o izboru, kandidat koji nije izabran može podnijeti zahtjev za uvid u dokumentaciju u vezi sa provedenom procedurom prijema u radni odnos.

Poslodavac će najkasnije u roku od tri dana o dana prijema zahtjeva omogućiti kandidatu uvid u dokumentaciju u vezi sa provedenom procedurom prijema u radni odnos, osim dokumentacije koja se odnosi na lične podatke drugih kandidata.

Kandidat kojem u ovom roku ne bude omogućen uvid u dokumentaciju, može zatražiti da fed.insp.rada izvrši inspekcijski nadzor.

NIJE propisan rok u kojem se može tražiti uvid.

-do okončanja postupka, tj. pravomoćnosti rješenja o prijemu izabranog kandidata (objektivni rok),

-do isteka roka za prigovor (subjektivni rok) imajući u vidu član 14. Uredbe prema kojoj kandidat koji je nezadovoljan odlukom iz člana 12. stav (4) Uredbe može u roku od 8 dana od dana prijema obavijesti izjaviti prigovor poslodavcu.

Omogućavanje uvida uz prethodno prekrivanje onih osobnih podataka izabranog kandidata koji se nalaze na službenim dokumentima ili na biografiji a koji nisu usko vezani uz provođenje konkursa i koji se odnose na privatnost izabranog kandidata (npr. JMBG, kontakt podaci - privatna adresa, privatni broj telefona/mobitela, datum i mjesto rođenja i sl.).

Uvid uz nadzor ovlaštene osobe se podrazumijeva.

Evidencije koje sadrže LP

Personalna evidencija obuvata:

- evidenciju o zaposlenim radnicima,
- evidenciju o platama,
- evidenciju o nesrećama na poslu,
- evidenciju radnika - matična knjiga,
- evidenciju drugih lica angažovanih na radu,
- evidenciju o radnom vremenu,
- elektronsku bazu podataka o radnicima,
- personalni dosije radnika.

Zaštitne mjere i odstupanja u vezi s obradom ličnog podatka u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe

Na obradu ličnih podataka u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili istorijskog istraživanja ili u statističke svrhe primjenjuju se odgovarajuće zaštitne mjere u skladu sa ZZLP u pogledu prava i sloboda nosioca podataka.

Zaštitnim mjerama osigurava se primjena tehničkih i organizacionih mjera, posebno onih kojima se garantira primjena principa smanjenja opsega podataka, koje mogu uključivati pseudonimizaciju, ako se svrhe mogu ostvariti tako.

Ako se svrhe mogu postići daljnjom obradom koja ne omogućava ili više ne omogućava identifikaciju nosioca podataka, te svrhe se ostvaruju na taj način.

Ako se lični podaci obrađuju u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih iz čl. 17, 18, 20. i 23. ZZLP, uz primjenu uslova i mjera zaštite iz stava (1), ako je vjerovatno da bi ta prava mogla spriječiti ili ozbiljno ugroziti ostvarivanje tih posebnih svrha, pa su takva odstupanja neophodna za njihovo postizanje.

Ako se lični podaci obrađuju u svrhu arhiviranja u javnom interesu, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih u čl. 17, 18, 20, 21, 22. i 23. ZZLP, uz primjenu uslova i mjera zaštite iz stava (1) tog člana, ako je vjerovatno da bi ta prava mogla spriječiti ili ozbiljno ugroziti ostvarivanje te posebne svrhe, pa su takva odstupanja neophodna za njeno postizanje.

Ako obrada iz st. (2) i (3) čl. 56. istovremeno služi i drugoj svrsi, odstupanja se primjenjuju samo za obradu u svrhe koje su navedene u tim stavovima.

BIOMETRIJA

Pojam biometrija je nastao od grčke riječi *bios* što znači život i *metrikos* što označava mjeru.

Biometrija je nauka prepoznavanja pojedinca koja se zasniva na identifikovanju ponašanja i bioloških karakteristika pojedinog lica, kao što su otisci prstiju, glas, hod, lice, šarenica oka i sl.

Najraširenija upotreba biometrijskih podataka je prisutna kod izdavanja putnih isprava. Prilikom podnošenja zahtjeva za izdavanje putne isprave, uzimaju se sljedeći biometrijski podaci podnosioca zahtjeva:

1) fotografija,

2) otisci prstiju,

3) potpis.

Biometrijske karakteristike se dijele na:

- fiziološke kao što su **lice**, otisak prsta, geometrija dlana, šarenica oka, mrežnica, termogram lica i tijela, uho, miris, DNK;
- ponašajne kao što su potpis, glas, dinamika kucanja i **hod**.

Obrada biometrijskih podataka u svrhu sigurne identifikacije

BIOMETRIJSKI PODATAK

je lični podatak dobijen posebnom tehničkom obradom u vezi sa fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičkog lica koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica, kao što su fotografije lica ili daktiloskopski podaci;

Član 57a.

- Obrada biometrijskih podataka može se provoditi samo ako je propisana zakonom ili ako je nužna za zaštitu lica, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačnu i sigurnu identifikaciju korisnika usluga, uzimajući u obzir da ne prevladavaju interesi nosioca podataka koji su u suprotnosti s obradom biometrijskih podataka iz člana 57a.
- pravni osnov za obradu biometrijskih podataka nosioca podataka radi sigurne identifikacije korisnika usluga izričita je saglasnost takvog nosioca podataka data u skladu s odredbama ZZLP.

Obrada biometrijskih podataka u službenim prostorijama

- **Član 57b.**

Dopuštena je obrada biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija, ako je propisano zakonom ili ako se takva obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija, uz uslov da je zaposlenik dao izričitu saglasnost za takvu obradu biometrijskih podataka u skladu s odredbama ovog zakona.

Postojeća pravila o zaštiti ličnih podataka crkava i vjerskih zajednica

Ako crkve i vjerske zajednice primjenjuju sveobuhvatna pravila u vezi s obradom ličnih podataka, ta postojeća pravila mogu se i dalje primjenjivati uz uslov da se usklade s novim ZZLP.

Crkve i vjerske zajednice koje primjenjuju sveobuhvatna pravila nadzire Agencija, osim ako crkva ili vjerska zajednica ne formira poseban nezavisan nadzorni organ, uz uslov da ispunjava uslove utvrđene u DIJELU ČETVRTOM ZZLP.

Obaveza čuvanja profesionalne tajne

- **Član 59.**

Posebnim propisom može se utvrditi ograničenje Agencije iz člana 103. stav(1) tač.f) i g) u vezi s kontrolorom podataka ili obrađivačem koji, na osnovu posebnog propisa koji je donio nadležni organ, podliježu obavezi profesionalne tajne i drugim jednakovrijednim obavezama tajnosti, ako je to nužno i razmjerno kako bi se uskladilo pravo na zaštitu ličnih podataka s obavezom tajnosti.

Poseban propis primjenjuje se samo na lične podatke koje je kontrolor podataka ili obrađivač dobio kao rezultat ili primio tokom aktivnosti koja je obuhvaćena obavezom tajnosti.

Video-nadzor

Praćenje određenog prostora putem video-nadzora dopušteno je samo ako je to nužno za zaštitu lica i imovine i ako ne prevladaju interesi nosioca podataka.

Video-nadzorom mogu biti obuhvaćeni samo prostori ili dijelovi prostora čiji je nadzor nužan radi postizanja ove svrhe.

Uspostavljanje video-nadzora javno dostupnih objekata velikih površina, kao što su sportski objekti, zabavni centri, tržni centri ili parkirališta, ili vozila javnog prevoza, dopušteno je isključivo s ciljem zaštite života, zdravlja i slobode lica te imovine.

Kontrolor podataka koji obavlja video-nadzor dužan je da donese odluku koja će sadržavati pravila obrade s ciljem poštovanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako video-nadzor nije propisan zakonom.

Kontrolor podataka ili obrađivač dužan je da na vidnom mjestu istakne oznaku o video-nadzoru.

Oznaka o video-nadzoru sadrži sljedeće informacije:

1.da je prostor pod video-nadzorom,

2.podatke o kontroloru podataka, odnosno obrađivaču i

3.kontaktne podatke putem kojih nosilac podataka može ostvariti svoja prava.

Oznaka treba biti vidljiva najkasnije prilikom ulaska u vidokrug snimanja.

Kontrolor podataka ili obrađivač dužan je da, kod sistema video-nadzora javno dostupnih objekata, bilježi zapise o upotrebi sistema i da ih čuva najmanje 12 mjeseci.

Zapisi omogućavaju da se utvrdi datum i vrijeme te identitet lica koje je ostvarilo uvid u sistem video-nadzora.

Praćenje javnih prostora putem video-nadzora u svrhe iz člana 1. stava (1) tačke c) ZZLP dopušteno je samo ako je to propisano posebnim zakonom.

Za uspostavljanje video-nadzora u stambenim, odnosno poslovno-stambenim zgradama potrebna je saglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova. Video-nadzorom može se obuhvatiti samo pristup ulasku i izlasku iz stambene zgrade, te zajedničke prostorije u stambenim zgradama.

Obaveze kontrolora u javnom sektoru prema novom ZZLP

TEHNIČKE I ORGANIZACIONE MJERE

Tehničke i organizacione mjere zaštite ličnih podataka predstavljaju skup postupaka, tehnologija i pravila koje kontrolor (ili obrađivač) podataka primenjuje kako bi osigurao bezbjednost i poverljivost ličnih podataka, u skladu sa ZZLP.

Sve mjere treba da budu:

- ✓Primjerene riziku (na osnovu vrste i osjetljivosti podataka),
- ✓Proporcionalne svrsi obrade,
- ✓Redovno ažurirane i testirane kako bi bile efikasne u stvarnoj primjeni.

Tehničke mjere

U fizičkom prostoru primjenjuju se odgovarajuće mjere tehničke zaštite prostorija i opreme u kojima se vrši obrada ličnih podataka.

Svrha: onemogućiti neovlašten pristup i obradu istih.

Tehničke mjere zaštite ličnih podataka, između ostalog, obuhvataju:

-kontrolu pristupa prostorijama i opremi za obradu ličnih podatka,

-zaštitu od uništenja i oštećenja ličnih podataka i dr.

Pri automatskoj obradi ličnih podataka tehničke mjere zaštite ličnih podatka su:

- ✓jedinstveno korisničko ime i lozinka sastavljena od kombinacije minimum šest karaktera, brojeva ili slova;
- ✓automatska izmjena lozinke po utvrđenom vremenskom periodu koji ne može biti duži od šest mjeseci;
- ✓korisničko ime i lozinka će dozvoljavati pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka;….

Dodatno!

- **Enkripcija (šifrovanje)**
- **Kontrola pristupa**
  - Korišćenje korisničkih naloga, lozinki, autentifikacije u više faktora (MFA) i prava pristupa kako bi se ograničio pristup samo ovlašćenim licima.
- **Zaštita mreže i sistema**
  - Firewall, antivirus, antimalver softver, sistem za detekciju upada (IDS/IPS), VPN za udaljeni pristup itd.
- **Redovan backup (rezervne kopije)**
- **Pseudonimizacija i anonimizacija**
- **Vođenje logova (dnevnika aktivnosti)**

Organizacione mjere

uključuju pravila, procedure, obuke i odgovornosti unutar organizacije, a cilj im je da obezbijede odgovorno i zakonito upravljanje ličnim podacima.

Najčešće organizacione mjere:

1. Politike i procedure zaštite podataka

❖Donošenje internih akata koji definišu kako se podaci prikupljaju, obrađuju, čuvaju i brišu.

2. Obuka radnika

❖ Edukacija osoblja o obavezama u vezi sa zaštitom podataka, prepoznavanju bezbjednosnih rizika i postupanju u slučaju povrede podataka.

3. Dodeljivanje odgovornosti (npr. imenovanje sl. za zaštitu podataka - DPO)

❖Jasno definisane uloge i odgovornosti u vezi sa obradom i zaštitom podataka.

4. Procjena rizika i DPIA (Procjena uticaja na zaštitu podataka)

❖Identifikacija rizika po prava i slobode pojedinaca i preduzimanje mjera za njihovo ublažavanje.

5. Ugovori sa obrađivačima

❖Zaključivanje ugovora sa trećim stranama koje obrađuju podatke u ime kontrolora, uključujući obaveze u vezi sa zaštitom podataka.

6. Politike upravljanja incidentima

❖Procedure za prijavljivanje, reagovanje i obavještavanje u slučaju povrede podataka.

TEHNIČKA I INTEGRISANA ZAŠTITA PODATAKA – PRIVACY BY DESIGN I PRIVACY BY DEFAULT

Koji faktori se posmatraju kod uvođenja mjera?

- ✓ najnovija dostignuća,
- ✓ troškovi sprovođenja i
- ✓ priroda, obim, kontekst i svrhe obrade, i
- ✓ rizici različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica koji proizlaze iz obrade podataka.

Rizici:

Prilikom procjene odgovarajućeg nivoa bezbjednosti, u obzir se uzimaju prije svega rizici koje predstavlja obrada, a posebno rizici od:

- slučajnog ili nezakonitog uništenja,
- gubitka,
- izmjene,
- neovlašćenog otkrivanja ličnog podatka ili
- neovlašćenog pristupa ličnom podatku koji je prenesen, čuvan ili na drugi način obrađivan.

Mjere:

- ✓ pseudonimizacija i enkripcija ličnog podatka,
- ✓ mogućnost obezbjeđivanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sistema i usluga obrade,
- ✓ sposobnost blagovremenog ponovnog uspostavljanja dostupnosti ličnog podatka i pristupa njemu u slučaju fizičkog ili tehničkog incidenta,
- ✓ postupak redovnog testiranja, ocjenjivanja i procjene djelotvornosti tehničkih i organizacionih mjera za postizanje bezbjednosti obrade.

Privacy by design

Ovaj pojam / princip potiče iz 90-ih godina XX vijeka.

Osmislila ga je En Čavoukian, tadašnja kanadska povjerenica za slobodu informacija i zaštitu podataka pokrajine Otawa.

Svrha upotrebe ovog principa je da budu ispoštovana pravila zaštite podataka još od najranije faze projekta i da djeluje proaktivno i preventivno u smislu zaštite prava pojedinca.

Poštovanje ovog principa se primarno zahtijeva od kreatora i lica zaduženih za tehnički razvoj sistema.

Procjena proporcionalnosti tehičkih i organizacionih mjera zaštite

Proporcionalnost mjera treba procijeniti u odnosu na 4 bitna faktora:

1. stanje tehnike, odnosno tehnološki razvoj,
2. troškove sprovođenja i prirodu,
3. obim, kontekst i svrhe obrade,
4. Rizike u vezi sa obradom (u odnosu na različite nivoe vjerovatnoće i ozbiljnosti potencijalnih ugrožavanja prava i sloboda fizičkih lica).

Čl. 27 / 34. ZZLP – slično, a različito!

Praktična pitanja

1) Da li su konkretne informacije neophodne za ostvarenje svrhe?
2) Koliko dugo su potrebne informacije?
3) Kome su sve potrebne informacije?
4) Da li postoji mogućnost decentralizovanog čuvanja podataka i odvajanja podataka?

Privacy by default - čl. 27/2

Kontrolor podataka primjenjuje odgovarajuće tehničke i organizacione mjere kojima se obezbjeđuje da integrisanim načinom budu obrađeni samo lični podaci koji su neophodni za svaku posebnu svrhu obrade.

Ta obaveza se primjenjuje na sve prikupljene lične podatke, obim njihove obrade, rok njihovog čuvanja i njihovu dostupnost.

Tim se mjerama obezbjeđuje da lični podaci nisu automatski, bez intervencije fizičkog lica, dostupni neograničenom broju drugih fizičkih lica.

Primjer kršenja ovog principa

Profili korisnika koji su po difoltu otvoreni.

Isto je i sa fotografijama koje se postavljaju na FB koje ne bi smjele po difoltu biti dostupne široj javnosti, već da korisnici sami odrede s kim žele da ih podijele.

PSEUDONIMIZACIJA

je obrada ličnog podatka tako da se lični podatak više ne može pripisati određenom nosiocu podataka bez korišćenja dodatnih informacija, uz uslov da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacionim mjerama kako bi se obezbijedilo da se lični podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

Smatraju se posredno utvrdivim LP

Funkcije pseudonimizacije

Ona podrazumijeva sakrivanje, odnosno “maskiranje” identiteta određene osobe.

Funkcije:

1)Zaštitna funkcija

2)Funkcija umanjenja količine podataka

3)Služi i ostvarenju principa Privacy by design

4)Bezbjedna obrada LP

5)Smanjenje rizika po pogođene osobe

Anonimizacija

Nije direktno definisana niti regulisana ZZLP, ali prema recitalu 26. GDPR:

Načela zaštite podataka stoga se ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ili na osobne podatke koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi. Ova se Uredba stoga ne odnosi na obradu takvih anonimnih informacija, među ostalim za statističke ili istraživačke svrhe.

Kod anonimizacije dolazi do toga da se određeno lice ne može više ne može identifikovati.

Odn. To nije moguće bez:

Dodatnih troškova, vremena za identifikaciju i dr. obj. faktora.

Primjer

ime	pseudonim	posao	pol	Datum rođ.	predmet	škola
Niko Nikić	4750	nastavnik	M	15.6.1973.	Mat/fizika	SC
Jasna Minić	Xyz3254	nastavnica	Ž	20.8.1970.	Engl. jezik	Gimnazija
Juso Jusić	22458	nastavnik	M	17.1.1961.	Biologija/hemija	Med. škola
Kristina Avdić	JKTZZHG	nastavnica	Ž	5.9.1997.	Fizičko vaspitanje	OŠ .....

Primjer ps.

pseudonim	posao	pol	Datum rođ.	predmet	škola
4750	nastavnik	M	15.6.1973.	Mat/fizika	SC
Xyz3254	nastavnica	Ž	20.8.1970.	Engl. jezik	Gimnazija
22458	nastavnik	M	17.1.1961.	Biologija/hemija	Med. škola
JKTZZHG	nastavnica	Ž	5.9.1997.	Fizičko vaspitanje	OŠ .....

Primjer an.

ime	posao	pol	Datum rođ.	predmet	škola
	nastavnik	M		Mat/fizika	SC
	nastavnica	Ž		Engl. jezik	Gimnazija
	nastavnik	M		Biologija/hemija	Med. škola
	nastavnica	Ž		Fizičko vaspitanje	OŠ .....

Korisno!

- Uputstvo za anonimizaciju sudskih odluka VSTS/V BIH

- Dostupno na https://portalfo2.pravosudje.ba/vstvfo-api/vijest/download/76324

ENKRIPCIJA

ili šifrovanje je proces pretvaranja podataka u nečitljiv oblik kako bi im pristup imale samo ovlašćene osobe ili sistemi.

Njena osnovna svrha je zaštita povjerljivosti informacija – čak i ako neovlašćena osoba dođe do šifrovanih podataka, neće moći da ih razumije bez ključa za dešifrovanje.

Vrste enkripcija

- ✓ Enkripcija slanja odn. prenosa podataka
- e-mail serveri
- Messaging usluge
- Platforme za saradnju sa trećim licima (npr. WebEx)
- Web stranice (npr. HTTPS protokol)
- LAN i VPN veze sa internim serverima
- ✓ Enkripcija snimanja odn. Čuvanja podataka
- Posebni fajlovi
- Datoteke
- Pojedine komponente računara (npr. hard diskovi)
- Prenosni medijumi (npr. USB)
- Cijeli operativni sistem

EVIDENCIJA O OBRADI LP

Šta je cilj?

POKAZATI USKLAĐENOST SA ZZLP

Kako?

Čl. 32. ZZLP propisuje obavezan sadržaj ove evidencije koji je različit za:

- Kontrolora i
- Obrađivača.

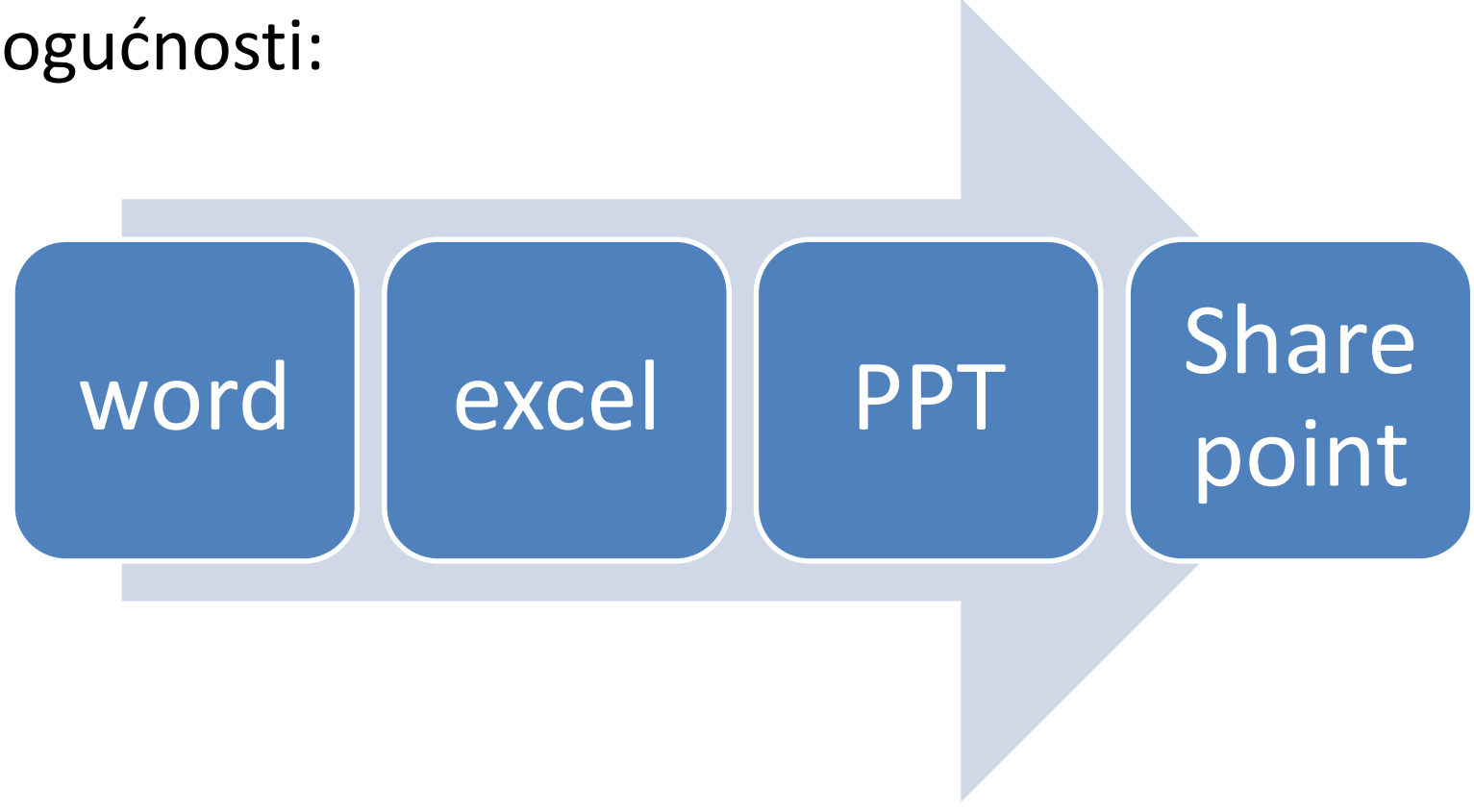
Sadržaj evidencije

1) Podaci o kontroloru
2) Podaci o obrađivaču
3) Svrsi i vrsti obrade
4) Vrsti lica na koje se podaci odnose
5) Vrsti podataka
6) Primaocima ili trećoj strani kojoj će podaci biti ustupljeni
7) Prenosu
8) Mjerama zaštite, ajp
9) I dr.

Forma evidencije

Evidencija mora biti u pisanoj formi, što uključuje i elektronsku formu.

Mogućnosti:



1

- Na zahtjev AZLP

2

- Kontrolor/obrađivač su dužni omogućiti uvid

3

- PREPORUKA: voditi je u fizičkom obliku (može el. Uz mogućnost štampanja)

Izuzeci od vođenja evidencije

Privredni subjekat ili organizacija u kojoj je zaposleno manje od **250 lica**, osim:

- ✓kada postoji vjerovatnoća da će obrada koju obavlja predstavljati visok rizik za prava i slobode nosioca podataka,
- ✓ako obrada nije povremena ili
- ✓ako obrada obuhvata posebne kategorije podataka iz člana 11. stava (1) ZZLP, ili su u pitanju lični podaci koji se odnose na krivičnu osuđivanost i krivična djela.

Evidencija kontrolora

Svaki kontrolor podataka i predstavnik kontrolora podataka, AJP, vodi evidenciju aktivnosti obrade za koje je odgovoran.

Evidencija sadrži sljedeće informacije:

a) ime i kontakt podatke kontrolora podataka i, AJP, zajedničkog kontrolora podataka, predstavnika kontrolora podataka i službenika za zaštitu podataka;

b) svrhe obrade;

c) opis kategorija nosilaca podataka i kategorija ličnih podataka;

d) kategorije primalaca kojima su lični podaci otkriveni ili će im biti otkriveni, uključujući i primaoce u drugim državama ili međunarodnim organizacijama;

e) AJP, o prenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, uključujući identifikaciju druge države ili međunarodne organizacije i, u slučaju prenosa iz člana 51. stava (2) ZZLP, dokumentaciju o odgovarajućim zaštitnim mjerama;

f) ako je moguće, predviđene rokove za brisanje različitih kategorija podataka;

g) ako je moguće, opšti opis tehničkih i organizacionih bezbjednosnih mjera iz člana 34. stava (1) ZZLP.

Evidencija obrađivača

I Kao kontrolor za svoje podatke

II

Svaki obrađivač i predstavnik obrađivača, AJP, vodi evidenciju o svim aktivnostima obrade koje se obavljaju u ime kontrolora podataka, koja sadrži:

a) ime i kontakt podatke jednog ili više obrađivača i svakog kontrolora podataka u čije ime obrađivač djeluje te, AJP, predstavnika kontrolora podataka ili obrađivača, kao i službenika za zaštitu podataka;
b) vrste obrade koje se obavljaju u ime svakog kontrolora podataka;
c) ako je primjenjivo, informacije o prenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, s identifikacijom te druge države ili međunarodne organizacije i u slučaju prenosa iz člana 51. stava (2) ZZLP, dokumentaciju o odgovarajućim zaštitnim mjerama;
d) ako je moguće, opšti opis tehničkih i organizacionih bezbjednosnih mjera iz člana 34. stava (1) ZZLP

POSTUPANJE U SLUČAJU POVREDE PODATAKA

Decembar 2022.

https://www.jutarnji.hr/vijesti/hrvatska/procurili-osobni-podaci-77-tisuca-hrvatskih-gradana-azop-otvorio-istragu-15286797

Januar 2024. godine

https://capital.ba/hakeri-zakljucali-izis-i-poslali-poruku-fondu-za-bezbolno-rjesenje/

https://www.nezavisne.com/novosti/ex-yu/Najveci-bezbjednosni-incident-u-istoriji-Hrvatske-Procurili-licni-podaci-181000-gradjana/764869

https://www.alo.rs/vesti/svet/1115076/licni-podaci-gradjana-svedske-osvanuli-na-dark-netu/vest

- Lični podaci više od milion građana Švedske objavljeni su na darknetu, izjavio je ekspert za sajber bezbednost, Karl Emil Nika, prenose danas švedski mediji.
- Tome je prethodio sajber upad u avgustu na čijoj meti su se našli sistemi firme Miljodata koja oprema čak 80 odsto švedskih lokalnih zajednica sistemima za upravljanje ljudskim resursima, prenosi nacionalna televizija SVT.

Definicija povrede LP

kršenje bezbjednosti koje dovodi do slučajnog ili nezakonitog:

- uništenja,
- gubitka,
- izmjene,
- neovlašćenog otkrivanja ili
- pristupa ličnim podacima koji su preneseni, čuvani ili na drugi način obrađivani.

U slučaju povrede kontrolor/obrađivač preduzima sljedeće:

Pravovremeno utvrđivanje povrede

Organizacione i tehničke mjere iz čl. 34. ZZLP imaju za cilj da obezbijede odgovarajući nivo bezbjednosti LP što podrazumijeva:

- ✓Sposobnost detekcije,
- ✓Adresiranja, i
- ✓Blagovremenog prijavljivanja povreda bezbjednosti.

Vrste povreda:

1. Povreda povjerljivosti
2. Povreda integriteta
3. Povreda dostupnosti

1+2+3
1+2
1+3
2+3

Obaveza obavještavanja AZLP

Kontrolor podataka dužan je da o povredi ličnog podatka bez nepotrebnog odgađanja i, ako je moguće, najkasnije u roku od 72 sata nakon saznanja za tu povredu obavijesti Agenciju o povredi ličnog podatka, osim u slučaju ako je vjerovatno da ta povreda neće ugroziti prava i slobode fizičkog lica. Ako izvještavanje nije izvršeno u roku od 72 sata, kontrolor podataka dužan je da Agenciji navede razloge za kašnjenje.

Obrađivač je dužan da, po saznanju za povredu ličnog podatka, bez nepotrebnog odgađanja o tome obavijesti kontrolora podataka.

Obaveza obavještavanja nosioca podatka

Kontrolor podataka dužan je da bez odgađanja pisanim putem obavijesti nosioca podataka o povredi ličnog podatka, ako je vjerovatno da će povreda ličnog podatka prouzrokovati visok rizik za prava i slobode fizičkog lica.

Kontrolor podataka u ovom obavještenju, jasnim i jednostavnim jezikom, opisuje prirodu povrede ličnog podatka te se najmanje navode informacije i mjere:

- ✓ime i prezime te kontakt podatke službenika za zaštitu podataka ili druge kontakt tačke od koje se može dobiti još informacija;
- ✓opis moguće posljedice povrede ličnog podatka;
- ✓opis mjera koje je kontrolor podataka preduzeo ili čije je preduzimanje predložio radi rješavanja problema povrede ličnog podatka, uključujući prema potrebi i mjere za ublažavanje njenih mogućih štetnih posljedica.

Kanali komunikacije

- Poštom – ako to nije povezano sa nesrazmjernim naporima
- E-mail
- SMS
- Web stranica kontrolora
- Istaknute reklame u štampanim medijima

Kad obavještavanje nije obavezno?

- ako je kontrolor podataka preduzeo odgovarajuće tehničke i organizacione zaštitne mjere i te mjere su primijenjene na lični podatak u vezi s kojim je došlo do povrede ličnog podatka, a prije svega mjere koje lični podatak čine nerazumljivim licu koje nije ovlašćeno da mu pristupi, kao što je enkripcija;
- ako je kontrolor podataka preduzeo naknadne mjere kojima se obezbjeđuje da više nije moguće da će doći do visokog rizika za prava i slobode nosioca podataka;
- ako bi to zahtijevalo neproporcionalan napor, mora se objaviti javno saopštenje ili se preduzima slična mjera kojom se nosioci podataka obavještavaju na jednako djelotvoran način.

Dokumentovanje svih aktivnosti

Obaveza proizilazi iz člana 35. st. 5. ZZLP

Kontrolor podataka dokumentuje:

- ✓ svaku povredu ličnog podatka,
- ✓ uključujući i činjenice u vezi sa povredom ličnog podatka, njene posljedice i
- ✓ mjere preduzete za otklanjanje štete.

Rok čuvanja ovih evidencija nije propisan.

Kontrolor određuje primjeren period čuvanja.

SLUŽBENIK ZA ZAŠTITU LIČNIH PODATAKA

Kontrolor podataka i obrađivač dužni su da imenuju službenika za zaštitu ličnih podataka u slučajevima:

- ako obradu obavlja javni organ, osim sudova koji postupaju u okviru sudske nadležnosti;
- ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od postupaka obrade koje zbog svoje prirode, obima i/ili svrhe zahtijevaju redovno i sistemsko praćenje nosioca podataka u velikom broju, ili
- ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od obimne obrade posebnih kategorija podataka na osnovu člana 11. ZZLP i ličnih podataka u vezi sa krivičnom osuđivanošću i krivičnim djelima iz člana 12. ZZLP.

Službenik za zaštitu ličnih podataka (eng. skr. DPO) imenuje se na osnovu njegovih stručnih kvalifikacija, a posebno **stručnog znanja o pravu i praksi u oblasti zaštite ličnih podataka** i sposobnosti obavljanja zadataka propisanih članom 41. ZZLP.

Službenik za zaštitu ličnih podataka može da bude zaposlen kod kontrolora ili obrađivača ili može da obavlja poslove na osnovu ugovora o djelu.

Kontrolor ili obrađivač objavljuje kontakt podatke službenika za zaštitu ličnih podataka i dostavlja ih AZLP.

DPO nije odgovoran za usklađenost, to je i dalje kontrolor/obrađivač!

Primjer kad se mora imenovati DPO

Privatno preduzeće koje se bavi bezbjednošću i nadzire više trgovačkih centara i javnih prostora. Nadzor je osnovna djelatnost tog preduzeća, što je nerazdvojno povezano sa obradom LP. Zato ovo preduzeće mora da imenuje DPO.

Polazi se od osnovne djelatnosti subjekta

Primjer kad se ne mora imenovati DPO

Sve organizacije koje obavljaju određene djelatnosti, kao što je isplata plata radnicima ili imaju standardnu IT podršku, kojima je to pomoćna djelatnost uz neku drugu osnovnu.

Ugovor o radu DPO

Pored obaveznih elementa ugovora o radu iz člana 35. stav 2. ZOR RS/24. st. 1. ZOR FBIH i ZOR BD BIH, ugovor o radu službenika za zaštitu LP treba da sadrži :

- Odredbu da službenik za zaštitu ličnih podataka, u vezi s obavljanjem svojih zadataka, dužan je da sve podatke do kojih dođe u postupku obrade podataka čuva kao službenu tajnu u skladu sa zakonom.

Opciono u ugovoru mogu biti navedeni zadaci službenika – posebno ako poslodavac nije u obavezi da donese akt o sistematizaciji.

Zadaci iz čl. 41. st.1. ZZLP

Akti kontrolora u javnom sektoru prema novom ZZLP

ODNOS PRAVILNIKA O ZAŠTITI LIČNIH PODATAKA I KODEKSA PONAŠANJA

Pravilnik o zaštiti ličnih podataka je **interni** akt koji donosi svaki **kontrolor** ili **obrađivač** ličnih podataka kako bi osigurao zakonitu i sigurnu obradu podataka.

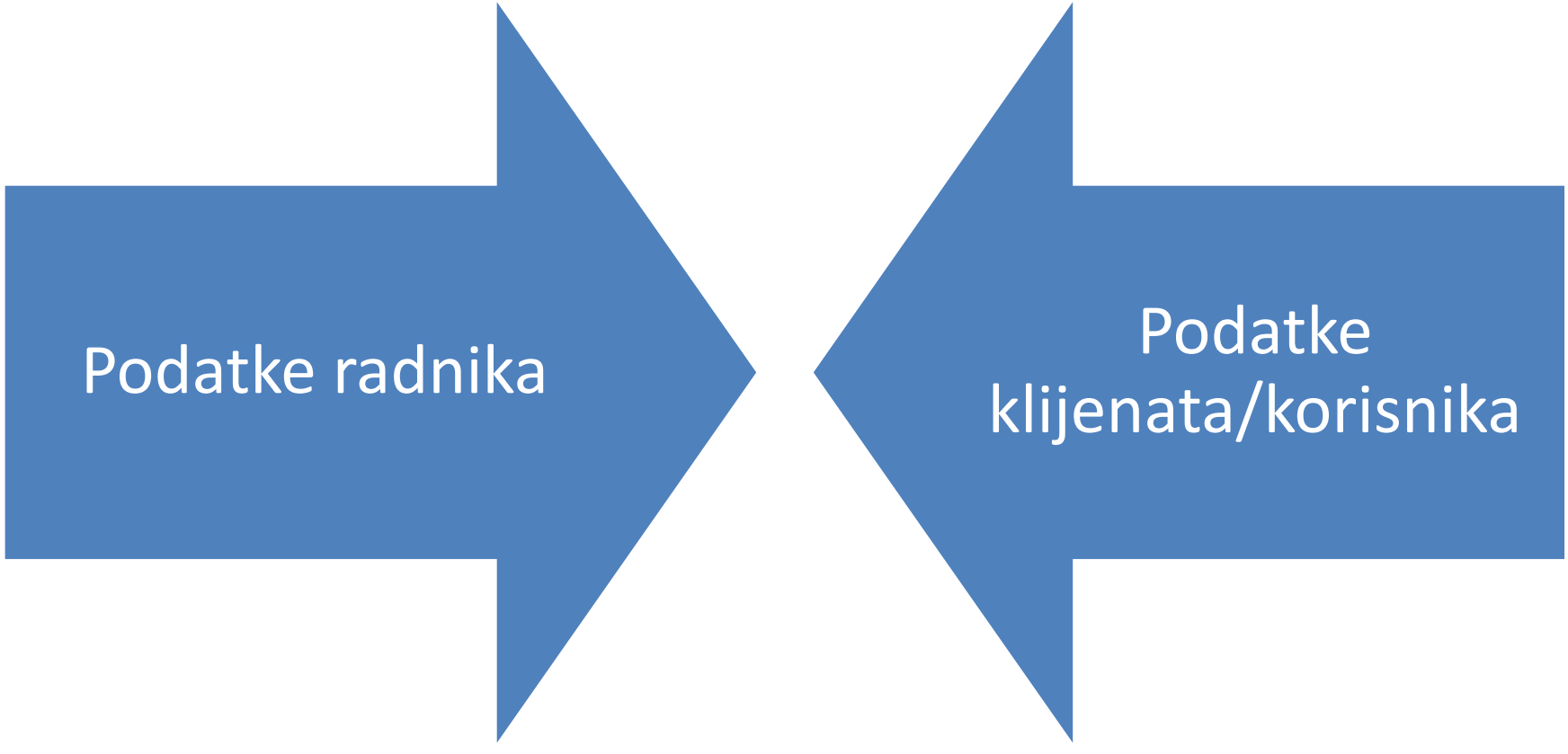
Kodeks ponašanja je akt koji donosi kontrolor ili obrađivač nakon što od AZLP dobije mišljenje da je nacrt kodeksa ponašanja u skladu sa ZZLP.

Pravilnik o ZLP je krovni dokument / donosi se prvi.

Posredno se zasniva na definiciji iz člana 4. tačka z) ZZLP

"obavezujuće poslovno pravilo" su **politike zaštite ličnih podataka kojih se kontrolor podataka i obrađivač** sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini **pridržava** prilikom prenosa ili skupova prenosa ličnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih država u okviru grupe privrednih subjekata ili grupe privrednih subjekata koji se bave zajedničkom privrednom djelatnošću.

Pravilnik se odnosi na svaku obradu LP u okviru kontrolora ili obrađivača što znači da pokriva 2 vrste podataka.



SVRHA PRAVILNIKA

Prati stvarnost i uređuje poslovanje onako kako je to zakonski ispravno i u skladu sa interesom poslovnog subjekta.

Njegova svrha je da približi načela na konkretnu situaciju kod konkretnog kontrolora ili obrađivača.

Razlikuje se kod različitih subjekata u jednom dijelu zavisno od konkretne djelatnosti koju obavlja, dok je glavnina normi identična.

PRAVILNIK O ZAŠTITI LIČNIH PODATAKA

donosi se sa ciljem usklađivanja sa važećim zakonodavstvom u oblasti zaštite LP.

Pravilnik definiše:

- principe,
- mjere i
- postupke koje subjekt primenjuje u prikupljanju, obradi, čuvanju i zaštiti ličnih podataka radnika, klijenata, korisnika usluga i drugih lica čiji se podaci obrađuju.

Cilj ovog dokumenta je da obezbedi zakonitu, poštenu i transparentnu obradu podataka, kao i da zaštiti prava i slobode fizičkih lica u vezi sa obradom njihovih podataka.

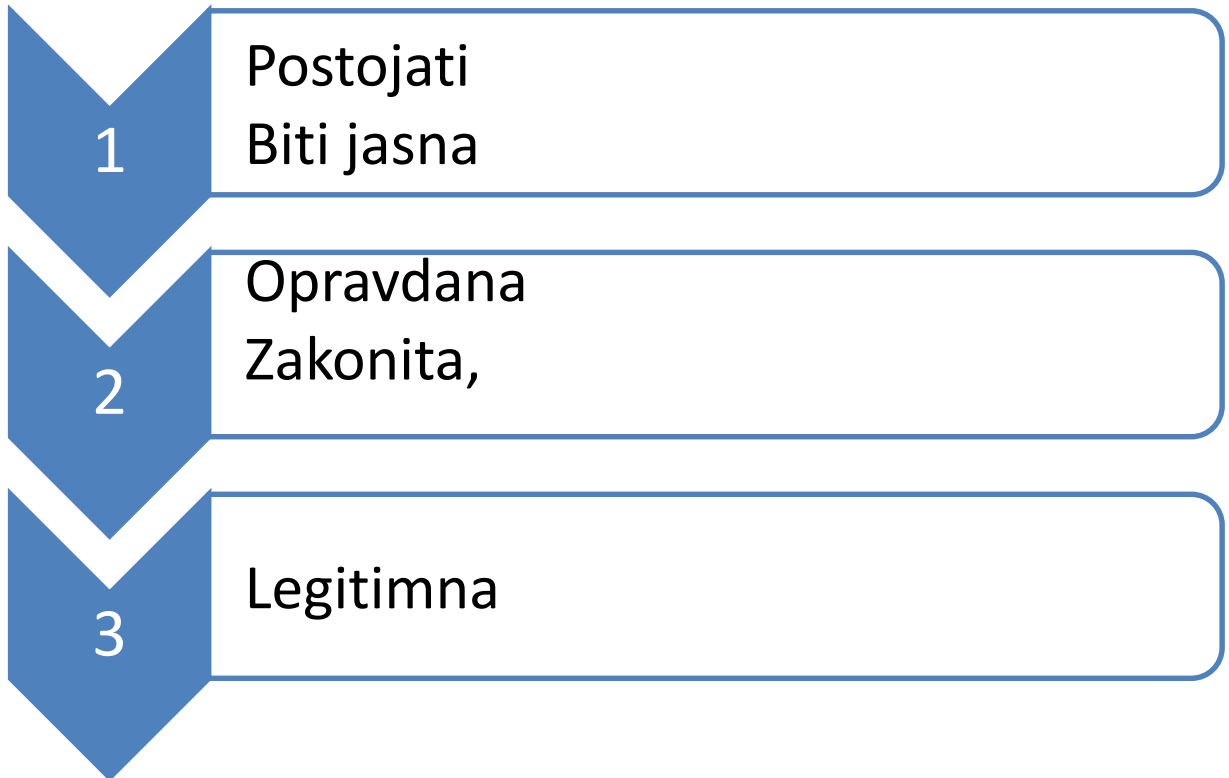
SVRHA OBRADE PODATAKA

Razlog obrade?

Primjer:

Vođenje zdravstvenog kartona radi pružanja medicinskih usluga i dijagnostike.

Svrha mora:



SADRŽAJ PRAVILNIKA

- Uvodne/opšte odredbe
- Osnovni pojmovi (opciono)
- Vrste podataka (mapiranje)
- Svrha prikupljanja/obrade podataka
- Pravni osnov obrade podataka
- Izvori ličnih podataka
- Prava nosioca LP
- Zapošljavanje i LP
- LP u digitalnoj formi
- Rokovi čuvanja podataka,

- Obaveze radnika u procesu obrade
- Prava lica čiji se podaci obrađuju
- Status lica zaduženog za zaštitu LP
- Evidencije obrade LP
- Video-nadzor
- Informacione tehnologije
- Ustupanje podataka trećim licima
- Izvoz podataka
- Mehanizmi zaštite
- Ostale odredbe

PRAVA NOSIOCA PODATAKA

1. Pravo na informisanje (čl. 15. i 16. ZZLP)
2. Pravo vlasnika podataka na pristup (čl. 17.)
3. Pravo na ispravku (čl. 18.)
4. Pravo na brisanje - „pravo na zaborav” (čl.19.)
5. Pravo na ograničenje obrade (čl.20.)
6. Pravo na prenosivost ličnih podataka (čl. 22.)
7. Pravo na prigovor (čl. 23.)
8. Pravo u vezi sa automatizovanim pojedinačnim donošenjem odluke, uključujući i profilisanje (čl. 24.)

Zašto ova prava trebaju biti sadržana u Pravilniku?

Kako bi se obezbijedilo osiguravanje prava nosioca podatka.

Jedan od načina je propisivanje obrazaca uz pravilnik.

Javni organi su dužni primjenjivati zakone o slobodi pristupa informacijama tako da u pravilnikom trebaju urediti davanje podataka o radnicima.

2. PROCJENA UTICAJA NA ZAŠTITU PODATAKA (DPIA)

Kontrolor prije obrade vrši procjenu uticaja predviđenih postupaka obrade na zaštitu ličnih podataka ako je vjerovatno da će ta obrada, posebno uzimajući u obzir nove tehnologije te prirodu, obim, kontekst i svrhe obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica.

Jedna procjena može se odnositi na više sličnih obrada koji predstavljaju slične visoke rizike.

Procjena uticaja na zaštitu podataka je obavezna u slučaju:

❖ sistemske i obimne procjene ličnih aspekata u vezi sa fizičkim licima koja se zasniva na automatizovanoj obradi, uključujući profilisanje, i koja je osnova za donošenje odluka koje proizvode pravni učinak u odnosu na fizičko lice ili na sličan način značajno utiču na fizičko lice;

❖obimne obrade posebnih kategorija ličnih podataka iz čl. 11. st. (1) ili podataka koji se odnose na krivičnu osuđivanost i krivična djela iz člana 12. ZZLP , ili

❖sistemskog praćenja javno dostupnog područja u velikoj mjeri.

Procjena uticaja obuhvata najmanje:

- sistematski opis predviđenih postupaka obrade i svrha obrade, uključujući ako je primjenjivo, legitiman interes kontrolora;
- procjenu neophodnosti i proporcionalnosti postupaka obrade u odnosu na njihove svrhe;
- procjenu rizika za prava i slobode vlasnika podataka; i
- predviđene mjere za rješavanje rizika, što uključuje zaštitne mjere, bezbjednosne mjere i mehanizme za obezbjeđivanje zaštite ličnih podataka i dokazivanje usklađenosti s ovim Zakonom, uzimajući u obzir prava i legitimne interese vlasnika podataka i drugih uključenih lica.

Kad postoji rizik za prava i obaveze FL?

Kada obrada može da prouzrokuje fizičku, materijalnu ili nematerijalnu štetu, a posebno ako za obrada može da dovede do:

- Diskriminacije,
- Krađe identiteta,
- Finansijskog gubitka,
- Štete za ugled,
- Gubitka povjerljivosti LP zaštićenih poslovnom tajnom,
- Neovlašćenog obrnutog postupka pseudonimizacije,
- Ako se obrađuju posebne kategorije LP,
- Ako se procjenjuju lični aspekti, a posebno u vezi sa poslom, ekonomskim stanjem, zdravljem, ličnim sklonostima,
- Ako obrada obuhvata tzv. Big Data podatke i sl.

Primjer

Primjeri obrade	Mogući relevantni kriterij	Hoće li procjena učinka na zaštitu podataka vjerovatno biti potrebna?
Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacijski sistem)	-Osjetljivi podaci ili podaci vrlo lične prirode -Podaci koji se odnose na osjetlljive ispitanike -Opsežne obrade podataka	Da
Upotreba sistema nadzornih kamera za praćenje ponašanja vozača na autoputevima. Sistem pametne video analize za prepoznavanje registarskih oznaka	-Sistemsko praćenje -Inovativna upotreba ili primjena tehnoloških ili organizacionih rješenja	Da

Primjer II

Primjer obrade	Mogući relevantni kriterij	Hoće li procjena učinka na zaštitu podataka vjerovatno biti potrebna?
Internet stranice e-trgovine koja prikazuje reklame za dijelove oldtajmera, što obuhvata i ograničenu izradu profila na osnovu pregleda ili kupovine na vlastitoj internetskoj stranici	- procjena ili bodovanje	Ne

Korisno!

Smjernice o procjeni učinka za zaštitu podataka i utvrđivanje mogu li postupci obrade “vjerovatno prouzrokovati visok rizik” u smislu Uredbe 2016/679

DRUGI AKTI ZA PRIMJENU ZZLP

1. Odluka o imenovanju službenika za zaštitu ličnih podataka
2. Obavještenje o obradi podataka
3. Saglasnost za obradu podataka
4. Odluka o video-nadzoru
5. Ugovor između kontrolora i obrađivača
6. Procjena uticaja na zaštitu podataka (skr. DPIA)
7. Politika privatnosti (website)
8. Politika kolačića (website)
9. Interne procedure koje se odnose na određene organizacione i tehničke mjere.

ZAKLJUČAK

Novi ZZLP je praktično GDPR + tzv. Policijska direktiva za BIH.

Karakterišu ga:

- strožiji rokovi,
- veće kazne,
- nova prava građana i
- mnogo jasniji tehnički i organizacioni zahtjevi.

To pred javne organe kao kontrolore postavlja nove obaveze, a svrha današnje edukacije je da se predstavnici ovih organa i SZLP detaljno upoznaju sa obavezama.

ZAKLJUČCI/ PREPORUKE

☑ Imenovati službenika za zaštitu LP

Rok – 4.10.2025.

☑ Usklađivanje sa ZZLP – rok 2 godine

- Izrada svih akata
- procjena rizika i mjera za smanjenje rizika
- revidiranje ostalih akata

☑ Edukacije SZLP i ostalih službenika/namještenika

Interne i eksterne obuke
Rok – 2 godine / kontinuirano

EFFECTIVE
USER
CAF-EXCELLENCE LABEL

Kontakt informacije

033/ 552-040

obuka@adsfbih.gov.ba

Alipašina 6,
71000 Sarajevo Bosna i Hercegovina

Posjetite novu TMS stranicu:
skeniraj QR CODE