Bosna i Hercegovina
Federacija Bosne i Hercegovine
AGENCIJA ZA DRŽAVNU SLUŽBU

Danijela Radonić, MA

PRIMJENA ZAKONA O ZAŠTITI LIČNIH PODATAKA BIH



30/10/2025 | 9:00 -12:00

CILJEVI SASTANKA

- 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

- Osnovne odredbe i principi Zakona o zaštiti ličnih podataka
- Uloge i odgovornosti kontrolora podataka
- Obrada ličnih podataka po zahtjevu trećih lica
- Prava lica na koja se podaci odnose

M2 Primjena ZZLP u oblasti radnog/službeničkog prava

- Prava zaposlenih/državnih službenika u kontekstu zaštite njihovih ličnih podataka
- Obaveze kadrovskih službi
- Sigurnosne provjere zaposlenika (prije zaposlenja i periodične tijekom trajanja radnog odnosa)

M3 Tehničke i organizacione mjere

- Uloga službenika za zaštitu ličnih podataka
- Sigurnosne mjere i procjena rizika
- Postupanje u slučaju povrede sigurnosti 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

OSNOVNE ODREDBE I PRINCIPI 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.

ULOGE I ODGOVORNOSTI KONTROLORA PODATAKA

Kontrolor podataka je fizičko ili pravno lice, javni organ ili nadležni organ koji samostalno ili sa drugim određuje svrhe i sredstva obrade ličnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriterijumi za njegovo imenovanje propisuju se zakonom.

Zajednički kontrolori - Ako dva ili više kontrolora podataka zajednički odrede svrhe i načine obrade, smatraju se zajedničkim kontrolorima podataka.

Kontrolor podataka dužan je da primijeni odgovarajuće tehničke i organizacione mjere imajući u vidu prirodu, obim, okolnosti i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica, kako bi obezbijedio da se obrada obavlja u skladu s ZZLP i kako bi to mogao dokazati. Te mjere se prema potrebi preispituju i ažuriraju.

Mjere, ako su proporcionalne u odnosu na aktivnosti obrade, uključuju sprovođenje odgovarajućih politika zaštite podataka od kontrolora podataka.

Poštovanje odobrenih kodeksa ponašanja iz člana 42. ili odobrenih mehanizama sertifikacije iz člana 44. ZZLP može služiti kao elemenat za dokazivanje usklađenosti s obavezama kontrolora podataka.

Uloge kontrolora

Kontrolor ima više međusobno povezanih uloga:

a) Upravljačka uloga

- Definiše svrhu obrade (zašto se podaci obrađuju) i način obrade (kako se obrađuju).
- Donosi interne akte i procedure o zaštiti podataka.
- Odlučuje o pravnom osnovu obrade (saglasnost, ugovor, zakon, legitimni interes i dr.).

b) Organizaciona uloga

- Imenovanje službenika za zaštitu podataka (ako je to obavezno).
- Uspostavljanje sistema internih kontrola i nadzora nad obradom.
- Osiguravanje adekvatne obuke zaposlenih.

c) Koordinaciona uloga

- Usklađuje aktivnosti između različitih odjela (npr. IT, HR, pravni sektor).
- Sarađuje sa obrađivačima (npr. IT firmama, knjigovodstvenim servisima).
- Postupa po zahtjevima i pritužbama lica na koje se podaci odnose.d

d)Uloga u odnosu prema nadzornom organu

- Komunicira i sarađuje sa Agencijom za zaštitu ličnih podataka.
- Obavještava Agenciju o povredi podataka ako postoji rizik po prava lica.
- Postupa po rješenjima i preporukama nadzornog organa.

Odgovornosti kontrolora

- Odgovornost za zakonitost obrade
- Odgovornost za tehničke i organizacione mjere
- Odgovornost prema licima na koja se podaci odnose
- Odgovornost u slučaju povrede podataka

OBRADA LIČNIH PODATAKA PO ZAHTJEVU TREĆIH LICA

kada

kome i

pod kojim uslovima

kontrolor smije otkriti lične podatke nekome ko nije ispitanik?

Obrada ličnih podataka po zahtjevu trećih lica zahtijeva poseban oprez, jasno dokumentovanje i ograničen pristup.

Kontrolor mora uvijek poći od principa:

“Ne dostavljaj više nego što je nužno, ne dostavljaj bez osnova, i uvijek možeš dokazati da si postupao zakonito.”

Ko su treća lica?

Obrada ličnih podataka po zahtjevu trećih lica znači da se lični podaci koje kontrolor čuva ili obrađuje daju, otkrivaju ili na drugi način stavljaju na raspolaganje licima koja nisu:

- ✓ nosioca podatka (lica na koja se podaci odnose),
- ✓ ovlašteni radnici kontrolora,
- ✓ ugovorni obrađivači podataka.

Primjeri:

- druga institucija, sud ili organ traži uvid u podatke,
- treća kompanija traži podatke o korisniku,
- pojedinac traži podatke o drugom licu (npr. bračni drug, roditelj, advokat, novinar).

Pravni osnov za dostavljanje podataka:

Čl. 8. ZZLP

a) Saglasnost nosioca

- Ako nosilac izričito da **pismenu i dobrovoljnu saglasnost** da se njegovi podaci dostave određenom trećem licu (npr. potvrda o zaposlenju banci).

b) Zakon ili drugi propis/obaveza kontrolora

- Ako je dostavljanje propisano **zakonom** (npr. dostavljanje Poreskoj upravi, sudu, policiji, tužilaštvu).

c) Ugovorna obaveza

- Ako je obrada nužna radi **izvršenja ugovora** u kojem je ispitanik strana (npr. slanje podataka kurirskoj službi radi isporuke robe).

d) Zaštita vitalnih interesa ispitanika

- U hitnim situacijama (npr. medicinska intervencija, spašavanje života).

e) Legitimni interes kontrolora ili treće strane

- Ako kontrolor ima **legitimni interes** koji ne nadjačava prava i slobode ispitanika – uz obaveznu procjenu proporcionalnosti i dokumentovanje razloga.

Obaveza procjene zakonitosti zahtjeva

Prije nego što dostavi bilo kakve podatke, kontrolor mora:

- **Identifikovati podnosioca zahtjeva** (dokazati da je treće lice zaista ono za koje se predstavlja).
- **Utvrditi osnov zahtjeva** – da li je zahtjev zasnovan na zakonu, sudskom nalogu ili saglasnosti.
- **Ograničiti obim podataka** – dostaviti samo one podatke koji su **nužni** za svrhu zbog koje se traže.
- **Voditi evidenciju** o svakom takvom zahtjevu i dostavljanju podataka.

Razlika u odnosu na raniji ZZLP

Osnov (ranije)

Član 17.

(1) Kontrolor podataka ne može dati lične podatke trećoj strani prije nego što o tome obavijesti nosioca podataka. Ako nosilac podataka ne odobri davanje ličnih podataka, oni se ne mogu otkriti trećoj strani osim ako to nije u javnom interesu.

(2) Kontrolor ličnih podataka ovlašten je lične podatke dati na korištenje drugim korisnicima na osnovu pisanog zahtjeva treće strane ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene nadležnosti ili ostvarivanja zakonitih interesa trećih strana.

(3) Pisani zahtjev mora sadržavati svrhu i pravnu osnovu za korištenje ličnih podataka, te vrste ličnih podataka koji se traže.

(4) Zabranjeno je davanje ličnih podataka na korištenje drugim korisnicima za čiju obradu, odnosno korištenje nisu ovlašteni prema odredbama čl. 5. i 6. ovog Zakona, te ako je svrha za koju se lični podaci traže na korištenje suprotna odredbi člana 4. ovog Zakona.

(5) Kontrolor podataka vodi posebnu evidenciju o ličnim podacima koji su dati na korištenje trećoj strani ličnih podataka i svrsi za koju su lični podaci dati.

(6) Nosilac podataka ne može ostvariti pravo na blokiranje ili uništavanje ličnih podataka ako kontrolor ima obavezu da obradi podatke prema posebnom zakonu ili ako bi time bila narušena prava trećih lica.

sada

Član 25.

(Ograničenja)

(1) Na osnovu posebnog zakona koji se primjenjuje na kontrolora podataka i obrađivača može se ograničiti opseg prava i obaveza iz člana 7, čl. od 14. do 24. ovog zakona i člana 36. ovog zakona, ako odredbe tog zakona odgovaraju pravima i obavezama propisanim u čl. od 14. do 24. ovog zakona, ako se takvim ograničenjem poštuje suština osnovnih prava i sloboda i ako ono predstavlja neophodnu i proporcionalnu mjeru u demokratskom društvu za zaštitu:

a) državne bezbjednosti;

b) odbrane;

c) javne bezbjednosti;

d) sprečavanja, istrage, otkrivanja ili gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od prijetnji javnoj bezbjednosti i njihovo sprečavanje;

e) drugih važnih ciljeva od opšteg javnog interesa u Bosni i Hercegovini, a posebno važnog privrednog ili finansijskog interesa, što uključuje monetarna, budžetska i poreska pitanja, javno zdravstvo i socijalnu zaštitu;

f) nezavisnosti pravosuđa i sudskih postupaka;

g) sprečavanja, istrage, otkrivanja i gonjenja povrede etike u zakonski regulisanim profesijama;

h) nadzorne, inspekcijske ili regulatorne funkcije koja je, najmanje povremeno, povezana s izvršavanjem službenih ovlašćenja u slučajevima iz tač. od a) do e) i tačke g) ovog stava;

i) nosioca podataka ili prava i sloboda drugih;

j) ostvarivanja potraživanja u građanskim sporovima.

Porezna tajna (čl. 3. PU FBIH)

(4) Porezna tajna su sve informacije ili podaci o poreznom obvezniku kojima raspolažu porezni organi, izuzev:

- informacija i podataka za koje porezni obveznik u pisanom obliku izjavi da se ne smatraju poreznom tajnom;

- informacija i podataka datih u takvom obliku da se ne mogu povezati sa pojedinačnim poreznim obveznikom ili ga se na drugi način ne može identifikovati;

- podataka o naplati poreza koji se, prema odredbama ovog zakona, javno objavljuju.

- podataka o dospjelom a neplaćenom dugu poreznih obveznika ako se daju sredstvima javnog informiranja (naziv/ime poreznog obveznika, ID broj i ukupan iznos duga).

Porezne informacije i podaci koji se smatraju poreznom tajnom mogu se dati :

- organima nadležnim za poduzimanje mjera i aktivnosti sa ciljem utvrđivanja poreznih obaveza, odgovornosti za porezne prekršaje i porezna krivična djela ;

- stranim poreznim vlastima u skladu sa međunarodnim ugovorima i

- drugim licima uz pisani pristanak poreznog obveznika;

- Vladi Federacije Bosne i Hercegovine, Parlamentu Federacije Bosne i Hercegovine, Vladi kantona, Skupštini kantona, gradonačelniku, Gradskoj skupštini, općinskom načelniku, općinskom vijeću i svim federalnim organima uprave i upravnim organizacijama.

Obaveza procjene zakonitosti zahtjeva

Prije nego što dostavi bilo kakve podatke, kontrolor mora:

- **Identifikovati podnosioca zahtjeva** (dokazati da je treće lice zaista ono za koje se predstavlja).
- **Utvrditi osnov zahtjeva** – da li je zahtjev zasnovan na zakonu, sudskom nalogu ili saglasnosti.
- **Ograničiti obim podataka** – dostaviti samo one podatke koji su **nužni** za svrhu zbog koje se traže.
- **Voditi evidenciju** o svakom takvom zahtjevu i dostavljanju podataka.

Postupanje prema različitim vrstama trećih lica

a) Državni organi i institucije

- Kontrolor mora postupiti **u skladu sa zakonom** koji uređuje zahtjev (npr. Zakon o krivičnom postupku, Zakon o Poreskoj upravi).
- Obavezno se provjerava da li zahtjev sadrži **pravni osnov, predmet i svrhu** obrade.
- Ako organ nema zakonski osnov, kontrolor ima pravo **odbijanja zahtjeva**.

b) Privatne kompanije ili fizička lica

- Mogu dobiti podatke **samo uz saglasnost** nosioca ili ako postoji drugi legitimni osnov.
- Česti slučajevi: banke, osiguravajuće kuće, poslodavci, advokati, mediji.

c) Advokati i zastupnici

- Moraju dokazati **ovlaštenje za zastupanje** (punomoć).
- Dostavljanje se ograničava samo na podatke koji su potrebni za zastupanje interesa klijenta.

d) Mediji i novinari

- Obrada se dozvoljava samo ako je u skladu s pravom na slobodu izražavanja i informisanja, uz poštovanje **balansa između privatnosti i javnog interesa**.

Evidencija i transparentnost

Kontrolor mora voditi **evidenciju o dostavljanju podataka trećim licima**, koja sadrži:

- ✓ datum i broj zahtjeva,
- ✓ naziv i kontakt tražioca,
- ✓ pravni osnov dostavljanja,
- ✓ koje podatke je dostavio,
- ✓ ime službenika koji je postupio po zahtjevu.

Također, ispitanik ima pravo da bude **obaviješten** o tome kome su njegovi podaci otkriveni, osim ako bi to ugrozilo zakonski postupak (npr. istragu).

Kako postupiti u slučaju sumnjivog ili nejasnog zahtjeva?

1. Kontrolor treba da zahtijeva dodatna pojašnjenja ili dokumente od tražioca podataka.
2. Ako zahtjev i dalje nije jasan – odgađa dostavljanje dok se ne provjeri osnov.
3. Po potrebi, konsultuje Agenciju za zaštitu ličnih podataka ili službenika za zaštitu podataka (SZLP).

Odgovornost kontrolora

Kontrolor snosi punu odgovornost za svaku obradu po zahtjevu trećeg lica. Nepravilno dostavljanje podataka može predstavljati:

- povredu Zakona o zaštiti ličnih podataka,
- osnov za **novčanu kaznu** i **odgovornost za štetu** prema nosiocu podatka,
- osnov za disciplinsku odgovornost zaposlenog koji je postupao.

Primjer

U ovom predmetu tužilja je tvrdila da joj je Poreska uprava (kao organ javne vlasti) omogućila da se iz baze podataka pristupi njenim ličnim podacima iz poreske prijave, a da ti podaci — koji podležu obavezi čuvanja kao tajni — budu objavljeni u dnevnom listu „Alo“ u obliku ekran-fotografije aplikacije „lokalna poreska administracija“.

Sud je utvrdio da je Poreska uprava povrijedila pravo tužilje na privatnost jer nije na zakonit način obezbijedila čuvanje i obradu njenih ličnih podataka, kako je to propisano Ustavom, Zakon o zaštiti podataka o ličnosti i Zakon o poreskom postupku i poreskoj administraciji.

Sud je naglasio da nije bitno za uspostavljanje odgovornosti da li je precizno utvrđeno koje konkretno lice je omogućilo objavu – odgovornost organa se ustanovljuje zbog neadekvatnog sistema zaštite podataka.

PRAVA VLASNIKA PODATAKA

1. **Pravo na informisanje**
2. **Pravo vlasnika podataka na pristup**
3. **Pravo na ispravku**
4. **Pravo na brisanje - „pravo na zaborav”**
5. **Pravo na ograničenje obrade**
6. **Pravo na prenosivost ličnih podataka**
7. **Pravo na prigovor**

Pravo na informisanje

omogućava da nosilac podatka bude obavješten o svim aspektima obrade (svrha, kontrolor i drugi korisnici podatka, zakonska obaveza dostavljanja podataka na obradu i dr.). Transparentna informacija, komunikacija i način ostvarivanja prava nosioca podataka su detaljnije uređeni pravilima iz člana 14. novog ZZLP.

Kontrolor podataka treba da preduzme odgovarajuće mjere kako bi se nosiocu podataka pružile sve informacije za ostvarivanje prava na informisanje.

Informacije se pružaju u pisanoj formi ili na druge načine, uključujući i elektronsku formu kada je primjereno.

Ako nosilac podataka zahtijeva, informacije se mogu pružiti usmeno, uz uslov da je identitet nosioca podataka utvrđen drugim sredstvima.

Pravo pristupa ličnim podacima

Kontrolor podataka obavještava nosioca podataka o toku obrade njegovih podataka koju vrši kontrolor podataka ili obrađivač podataka:

- *o svrsi obrade podataka,*
- *zakonskoj osnovi i trajanju obrade,*
- *da li su podaci pribavljeni od nosioca podataka na njegov zahtjev ili od treće strane i*
- *o pravu na pristup ličnim podacima, kao i*
- *o tome ko je primio ili ko će primiti podatke i za koju svrhu*

naročito primaocima u trećim zemljama ili međunarodnim organizacijama.

Nosilac ima pravo dobiti od kontrolora obrade potvrdu obrađuju li se lični podaci koji se odnose na njega te ako se takvi lični podaci obrađuju, pristup.

Dodatna prava novi ZZLP

- ✓ kategorije ličnih podataka o kojima je riječ;
- ✓ pravo da se od kontrolora obrade zatraži ispravka ili brisanje ličnih podataka ili ograničavanje obrade ličnih podataka koji se odnose na nosioca ili prava na prigovor na takvu obradu;
- ✓ pravo na podnošenje prigovora AZLP;
- ✓ određena prava kod automatizovanog donošenja odluka;
- ✓ pravo na informisanje o odgovarajućim zaštitnim mjerama u skladu sa čl. 48. koje se odnose na prenos podataka u treću zemlju ili međunarodnu organizaciju.
- ✓ pravo na dobijanje kopije ličnih podataka.

Pravo pristupa ličnim podacima – novi Zakon

- svrsi obrade;
- kategorijama ličnih podataka koje se obrađuju;
- primaocima ili kategorijama primalaca kojima su lični podaci otkriveni ili će im biti otkriveni, a posebno primaocima u drugim državamaili međ. org.;
- predviđenom roku u kojem će se lični podaci čuvati, ako je to moguće, ili, ako to nije moguće, kriterijima za određivanje tog roka;
- pravu da se od kontrolora zatraži ispravka ili brisanje ličnih podataka ili ograničavanje obrade ličnih podataka koji se odnose na vlasnika podataka ili prava na prigovor na takvu obradu;
- pravu na podnošenje prigovora AZLP;

- ✓ ako se lični podaci ne prikupljaju od vlasnika podataka, svakoj dostupnoj informaciji o njihovom izvoru;
- ✓ postojanju automatizovanog donošenja odluka, uključujući i profilisanje iz člana 24. stav (1) i (4) te, najmanje u tim slučajevima, razumne informacije o logici koja se koristi, kao i značaju i predviđenim posljedicama takve obrade za vlasnika podataka;
- ✓ ako se lični podaci prenose u drugu državu ili međunarodnoj organizaciji, vlasnik podataka ima pravo da bude informisan o odgovarajućim mjerama zaštite u skladu sa članom 48. koje se odnose na prenos podataka;
- ✓ obezbjeđuje kopiju ličnih podataka koji se obrađuju.

Za sve dodatne kopije koje zatraži nosilac podataka, kontrolor može naplatiti opravdanu naknadu na osnovu administrativnih troškova.

Ako nosilac podataka podnese zahtjev elektronskim putem te osim ako nosilac ne zahtijeva drugačije, informacije se pružaju u uobičajenom elektronskom obliku.

Ispravljanje, brisanje i blokiranje podataka

Kontrolor će, na zahtjev nosioca podataka, ispraviti, izbrisati ili blokirati podatke za koje se utvrdi da su netačni ili da su pogrešno navedeni ili obrađeni na drugi način koji je suprotan zakonu i pravilima koji se odnose na obradu podataka.

Po zahtjevu nosioca podataka kontrolor obavijestiti treću stranu kojoj su podaci preneseni o ispravkama.

Pravo na ispravku

Nosilac podataka ima pravo da mu kontrolor omogući ispravku netačnih ličnih podataka, bez nepotrebnog odgađanja.

Uzimajući u obzir svrhu obrade, nosilac podataka ima pravo da dopuni nepotpune lične podatke, između ostalog i davanjem dodatne izjave.

Pravo na brisanje – pravo na zaborav

ako je ispunjen jedan od sljedećih uslova:

- lični podaci više nisu neophodni za svrhe u koje su prikupljeni ili na drugi način obrađeni;
- nosilac podataka je povukao saglasnost na kojoj je obrada zasnovana u skladu sa članom 8. stav (1) tačka a) ili članom 11. stav (2), tačka a) i ako ne postoji drugi pravni osnov za obradu;
- nosilac podataka je uložio prigovor na obradu u skladu sa članom 23. stav (1) i ne postoje preovlađujući zakonski razlozi za obradu, ili je vlasnik podataka uložio prigovor na obradu u skladu sa članom 23. stav (2);
- lični podaci su nezakonito obrađeni;
- lični podaci moraju biti obrisani radi postupanja u skladu sa zakonskom obavezom kojoj podliježe kontrolor;
- lični podaci su prikupljeni u vezi sa ponudom usluga informacionog društva iz člana 10. stav (1).

Pravo na ograničenje obrade

omogući ograničenje obrade ako je ispunjen jedan od sljedećih uslova:

- nosilac podataka osporava tačnost ličnih podataka, u roku u kojem se kontroloru omogućava da provjeri tačnost ličnih podataka;
- obrada je nezakonita, a nosilac podataka se protivi brisanju ličnih podataka i umjesto toga traži ograničenje njihove obrade;
- Kontroloru više nisu potrebni lični podaci za potrebe obrade, ali ih vlasnik podataka zahtijeva radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva;
- nosilac podataka je uložio prigovor na obradu u skladu sa članom 23. stav (1) i očekuje potvrdu da li njegovi razlozi preovladavaju legitimne razlogekontrolora.

Pravo na prenosivost LP

Nosilac podataka ima pravo da preuzme lične podatke koji se odnose na njega, a koje je dao kontroloru u strukturisanom, uobičajno upotrebljavanom i mašinski čitljivom formatu te ima pravo da prenosi te podatke drugom kontroloru bez ometanja od strane kontrolora kojem su lični podaci dati, ako:

- je obrada zasnovana na saglasnosti u skladu sa članom 8. stav (1) tačka a) ili članom 11. stav (2) tačka a) ili na ugovoru u skladu sa članom 8. stav (1) tačka b); i
- ukoliko se obrada vrši automatski.

Prilikom ostvarivanja svojih prava na prenosivost podataka nosilac podataka ima pravo na neposredni prenos od jednog kontrolora drugom kontroloru, ako je to tehnički izvodljivo.

Pravo na prigovor

Nosilac podatka u svakom trenutku kontroloru može podnijeti prigovor na obradu njegovih ličnih podataka, u skladu sa članom 8. stav (1) tačka e) ili f) uključujući profilisanje zasnovano na tim odredbama.

Kontrolor ne smije dalje obrađivati lične podatke, osim u slučaju:

- ✓ da dokaže da postoje uvjerljivi legitimni razlozi za obradu koji preovladavaju nad interesima, pravima i slobodama nosioca podataka ili
- ✓ radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

Pravo na prigovor – direktni marketing

Ako se lični podaci obrađuju za potrebe direktnog marketinga, nosilac podataka ima pravo da u bilo kojem trenutku uloži prigovor na obradu ličnih podataka za potrebe takvog marketinga, što uključuje profilisanje u mjeri u kojoj je povezano sa takvim direktnim marketingom.

Ako se nosilac podataka protivi obradi za potrebe direktnog marketinga, lični podaci više se ne smiju obrađivati u te svrhe.

Najkasnije u trenutku prve komunikacije sa nosiocem podataka, njemu se izričito mora skrenuti pažnja na ova prava, te se to mora učiniti na jasan način i odvojeno od bilo koje druge informacije.

Direktni marketing je "interaktivan sistem marketinga koji se koristi jednim ili više medija za oglašivanje kako bi se uticalo na mjerljiv odgovor i/ili transakciju na bilo kojoj lokaciji".

Ako se nosilac protivi obradi za potrebe direktnog marketinga, lični podaci se više ne smiju obrađivati u takve svrhe.

Automatizovano pojedinačno donošenje odluka

NOsilac podataka ima pravo da se na njega ne primjenjuje odluka zasnovana isključivo na automatizovanoj obradi, uključujući i profilisanje, koja proizvodi pravne efekte ili na sličan način značajno na njega utiču.

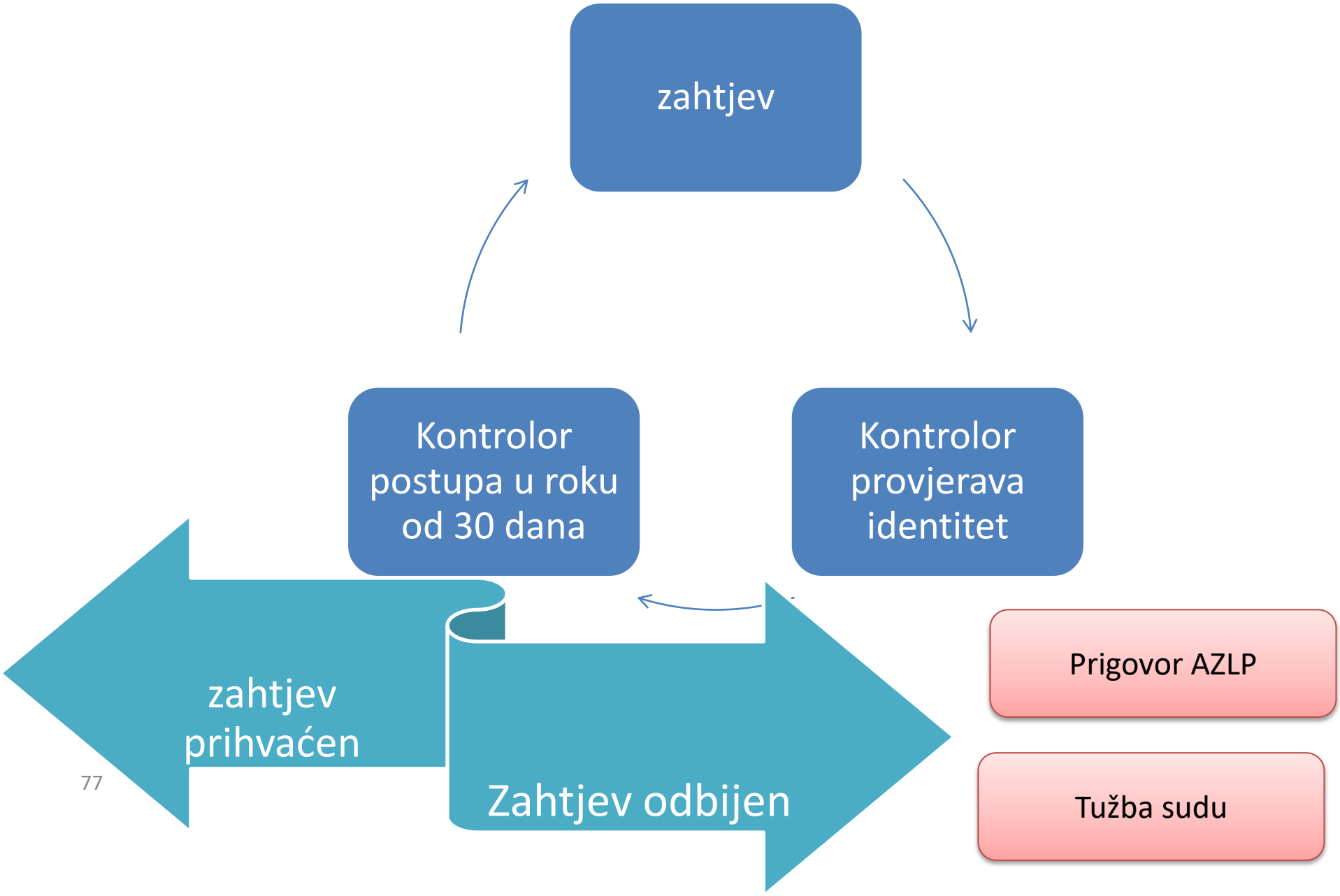
To se ne primjenjuje se ako je odluka:

- potrebna za zaključivanje ili izvršenje ugovora između nosioca podataka i kontrolora;
- dozvoljena zakonom koji se primjenjuje na kontrolora i koji propisuje odgovarajuće zaštitne mjere za prava i slobode te legitimne interese nosioca podataka; ili
- zasnovana na izričitoj saglasnosti nosioca podataka.

Kontrolor preduzima odgovarajuće mjere za zaštitu prava i sloboda te legitimnih interesa nosioca podataka, najmanje:

- **prava na učešće fizičkog lica u donošenju odluke,**
- **prava izražavanja sopstvenog stava i**
- **prava na osporavanje odluke.**

Kako nosilac vrši ostvarivanje svojih prava?



Ostvarivanje prava na pristup informacijama shodno ZSPI

1. Podnošenje zahtjeva nadležnom javnom organu.

   Zahtjev mora sadržavati osnovne podatke: koje informacije se traže, u kojm obliku, i kontakt podnositelja.

2. Organ je dužan da odluči o zahtjevu u roku 15 dana od prijema. Može:

a) odobriti pristup u cijelosti,

b) b) djelimično odobriti,

c) odbiti (uz obrazloženje i pozivanje na zak. razloge za ograničenje).

3. Način ostvarivanja prava:

- uvid u dokumenta,
- kopije u papirnom ili elektronskom obliku, ili
- usmene informacije.

Troškovi se mogu naplatiti samo za umnožavanje ili dostavu (ne i za sam pristup).

Pravni lijekovi za nosioca prava

Ako organ ne odgovori ili odbije zahtjev → nosilac prava može podnijeti žalbu.

Ako i dalje nije zadovoljan → može pokrenuti upravni spor pred sudom.

Posebna garancija

Zakon predviđa da se svako ograničenje pristupa mora tumačiti restriktivno i da se primjenjuje test javnog interesa (da li bi objava informacije donijela veću korist javnosti nego što bi štetila zaštićenom interesu).

Primjena ZZLP u oblasti radnog/službeničkog prava

Period obrade LP

- ✓ prije zasnivanja radnog odnosa – konkursna procedura
- ✓ tokom trajanja radnog odnosa
- ✓ po prestanku radnog odnosa

Posebna napomena!

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:

FBIH

- 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 od 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.

Koje podatke poslodavac ne smije tražiti od potencijalnog kandidata?

Najčešća greška je što poslodavci traže previše ličnih podataka koji nisu opravdani svrhom.

Nije dozvoljeno da budući poslodavac zahtjeva od kandidata:

- ✓ previše podataka,
- ✓ podatke koji nisu od uticaja na odluku o zapošljavanju, te
- ✓ podatke koji previše otkrivaju, kada je moguće dobiti potrebne informacije sa manje uplitanja,
- ✓ podatke o djeci (ime i datum rođenja).

Ukoliko poslodavac prikuplja podatke o potencijalnim radnicima direktno od njih (popunjavanjem prijave za posao) trebao bi naznačiti koji su podaci obavezni, a koji su dobrovoljni.

Za obavezne podatke poslodavac bi trebao navesti zakonski osnov.

Kako bi vlasniku ličnih podataka obezbijedio pravo na informisanje, poslodavac mora u ponudi za posao, oglasu ili na web stranici navesti sljedeće informacije:

- svoj identitet (puni naziv i adresa sjedišta);
- svrha prikupljanja ličnih podataka;
- primaoce ličnih podataka ili njihove kategorije, ukoliko su poznati na dan prikupljanja;
- pravo na pristup i pravo na ispravku ličnih podataka.

Pored toga, često poslodavci ne uništavaju podatke kandidata koje nisu izabrali, nego ih čuvaju za neki sljedeći konkurs, što nije zakonito osim ako je kandidat izričito dao saglasnost za to.

Pribavljanje dokaza o neosuđivanosti

Poslodavac ima pravni osnov za obradu podataka iz krivične evidencije, ali isključivo za lice koje se imenuje za direktora.

Međutim, način prikupljanja tih podataka od svih učesnika koji se prijavljuju na predmetni konkurs suprotan je odredbama Krivičnog zakona.

„Niko nema pravo da traži od građana da podnese dokaze o svojoj osuđivanosti ili neosuđivanosti.“

„Podaci iz krivične evidencije mogu se na obrazložen zahtjev dati državnim organima, preduzećima i drugim pravnim licima, ako još traju određene pravne posljedice osude ili mjere bezbjednosti ili ako za to postoji opravdan interes zasnovan na zakonu.“

Pribavljanje dokaza o nevođenju krivičnog postupka

Poslodavac može tražiti samo ako je zakonom propisano da je nevođenje krivičnog postupka uslov za izbor i imenovanje direktora.

Ako je zakonom propisano, dostavu uvjerenja ne treba tražiti od svih kandidata i u ovoj fazi konkursa.

To iz razloga što svi kandidati koji se prijavljuju na javni konkurs neće biti izabrani i imenovani za direktora. Zahtijevanje od svih kandidata da dostave uvjerenje o nevođenju krivičnog postupka predstavlja:

- ✓ bespravno uplitanje u njihovu privatnost kao i
- ✓ nepotrebno izlaganje troškovima.

OBRADA LIČNIH PODATAKA RADNIKA

čl. 30. ZOR FBIH

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.

Koje podatke prikuplja poslodavac?

Podatke koje poslodavci prikupljaju (u zakonite svrhe) možemo podijeliti na:

- podatke koji pomažu pri selekciji kandidata za zapošljavanje ili upućivanja radnika na obuke i usavršavanje;
- podatke koji su neophodni za obezbjeđivanje bezbjednosti i zdravlja na radu;
- podatke koji su im neophodni radi zaštite imovine;
- podatke koji služe za kontrolu rada;
- podatke koji su im potrebni radi ispunjavanja drugih zakonskih obaveza.

Koji podaci nisu od neposrednog značaja za posao?

- ✓ podaci koji mogu biti osnov za diskriminaciju (vjera, političko opredjeljenje, seksualna orjentacija, te drugi osnovi diskriminacije iz člana 2. Zakona o zabrani diskriminacije),
- ✓ podaci o trudnoći,
- ✓ podaci o hroničnim bolestima,
- ✓ disciplinskim mjerama kod drugih poslodavaca,
- ✓ razlogu za prestanak radnog odnosa kod prethodnih poslodavaca,
- ✓ u nekim djelatnostima podaci o posebnim krivičnim djelima nisu od neposrednog značaja (npr. u obrazovnim ustanovama se ne mogu zaposliti lica koja su pravnosnažno osuđena za krivična djela učinjena protiv dostojanstva ličnosti, morala, zloupotrebe opojnih sredstava, službene dužnosti, polnog integriteta, zlostavljanja djeteta, polnog i drugog nasilja nad djetetom ili maloljetnim licem, ali za druge poslodavce ova smetnja za zasnivanje radnog odnosa nije propisana).

PRIKUPLJANJE LP

Izvor ličnih podataka:

- Lično od radnika/radnice
- Treća strana

U slučaju prikupljanja podataka od treće strane, poslodavac je dužan:

- ✓ bez odgađanja obavijestiti radnika/radnicu o tome ko je treća strana koja je poslodavcu dostavila lične podatke, i
- ✓ osigurati informacije u skladu s članom 22. ZZLP.

Primjer: Rizici u kadrovskoj evidenciji

- Odavanje ličnih podataka zbog neadekvatne kontrole pristupa;
- Odavanje ličnih podataka od strane ovlaštenih lica;
- Neovlaštena izmjena ličnih podataka zbog neadekvatnih sigurnosnih mjera;
- Nekontrolisana izmjena ličnih podataka od strane ovlaštenog lica;
- Nedostupnost ličnih podataka zbog neadekvatnih tehničko-sigurnosnih mjera;
- Namjerno uništenje ličnih podataka od strane ovlaštenih lica.

POSTUPANJE SA LIČNIM PODACIMA NAKON PRESTANKA RADNOG ODNOSA

Šta vraća radniku?

Prema važećim propisima iz oblasti radnih odnosa poslodavac određene isprave vraća radniku prilikom prestanka radnog odnosa. To će biti lični dokumenti:

- kopija LK ili drugog identifikacionog dokumenta;
- diplome, certifikati i sl;
- uvjerenja javnih organa (uvjerenje o nevođenju krivičnog i/ili prekršajnog postupka, ljekarska uvjerenja);
- radnu knjižicu (u Republici Srpskoj);
- kopiju odjave kod Poreske uprave.

Poslodavac radniku vraća ove isprave jer prestankom radnog odnosa prestaje svrha vođenja ličnih podataka ovog radnika, a prestaje i pravni osnov za obradu.

Šta ne vraća radniku?

Poslodavac radniku ne vraća isprave i dokumente koje je radniku izdao u toku vođenja radnog odnosa:

- ✓ razna rješenja kojim se odlučuje o pravima radnika,
- ✓ naredbe i
- ✓ pojedinačna obavještenja i uputstva.

No i ove isprave ne može čuvati trajno, nego u skladu sa propisanim rokovima koji proizilaze iz propisa o arhivskoj djelatnosti.

Trajno čuva

Evidencije iz oblasti rada (podaci o zaposlenim radnicima, odnosno matična evidencija, podaci o platama, o nesrećama na radu) poslodavac je dužan da iste čuva trajno.

Evidenciju o prisustvu radnika na radu poslodavac ne čuva trajno:

- u Republici Srpskoj čuva najkraće dvije godine
- u Federaciji BIH je dužan čuvati najmanje pet godina.

a u slučaju kada poslodavac ima saznanja da je pokrenut radni spor u vezi sa ostvarivanjem prava iz radnog odnosa ili u vezi sa radnim odnosom, pri čemu bi za ostvarivanje tih prava mogle biti relevantne i evidencije, te evidencije čuva do pravosnažnog okončanja tog spora.

Dakle, čuvanje ovih evidencija predstavlja izuzetak od propisa o zaštiti ličnih podataka da se lični podaci čuvaju u formi koja dopušta identificiranje nosioca podataka ne duže nego što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju.

PRAVA ZAPOSLENIH/DRŽAVNIH SLUŽBENIKA U KONTEKSTU ZAŠTITE NJIHOVIH LIČNIH PODATAKA

(Obrada ličnih podataka u kontekstu zaposlenja)

Posebnim zakonom ili KU 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.

Ova pravila uključuju prikladne i posebne mjere za zaštitu:

- ✓ ljudskog dostojanstva nosioca podataka,
- ✓ njegovih legitimnih interesa i osnovnih prava, posebno u vezi sa transparentnošću obrade, prenosom ličnih podataka unutar grupe privrednih subjekata ili grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kao i
- ✓ sistemom praćenja na radnom mjestu.

Propisi o radu

- ZDS ne sadrži nijednu odredbu koja se odnosi na ZLP  potrebno uskladiti sa ZZLP
- čl. 30. ZOR FBIH

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.

Prava nosioca podatka u kontekstu zaposlenja

- Pravo na pristup
- Pravo na ispravku
- Pravo na brisanje
- Pravo na prigovor

OBAVEZE KADROVSKIH SLUŽBI

❖Mapiranje podataka:

Ime i prezime, JMBG, adresa, broj TR i podaci o zdravlju

Sagledati:

1. Pravni osnov
2. Svrhu obrade
3. Rokove čuvanja
4. Ko ima pristup podacima?

Ključne obaveze

- Dobijanje saglasnosti (kada se obrada ne zasniva na zakonu ili drugom pravnom osnovu)
- Informisanje zaposlenih
- Ograničenje pristupa → samo HR i obračun plata
- Vođenje evidencija
- Period čuvanja i arhiviranje

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.

Evidencija radnog vremena

Poslodavac je dužan da vodi dnevnu evidenciju o prisustvu radnika na radu.

U evidenciji je poslodavac dužan da navede vrijeme početka i završetka dnevnog rada radnika.

Pravilnik o sadržaju i načinu vođenja evidencije o radnicima i drugim licima angažovanim na radu ("SN FBiH", 92/2016) – čl. 8.-14.

Način vođenja evidencije radnog vremena

Podaci o radnom vremenu mogu se voditi pisano u obliku knjige ili u elektroničkom obliku i uz korištenje odgovarajućih kratica, ali uz odgovarajuće nedvojbeno i jasno pojašnjenje značenja svake kratice.

PRIKUPLJANJE PODATAKA:

- potpisivanje u svesku
- neposredna provjera
- očitavanje putem kartice ili čitača (RFID)
- softwer za evidenciju radnog vremena i kontrolu pristupa
- otisak prsta ili snimanje rožnjače (biometrija)– NIJE u skladu sa ZLP
- Sada može samo izuzetno čl. 57a. i 57b. ZZLP
- Kamere uz čitač?

https://kamir.net/index.php/usluge/evidencija-radnog-vremena

VIDEONADZOR POSLOVNIH PROSTORIJA

Svrha obrade:

- bezbjednost lica i imovine.

Putem videonadzora nosilac podatka se može identifikovati najmanje na dva načina:

1. direktno
Snimanjem lica
i/ili
2. indirektno
Snimanjem hoda

Zakonito postavljanje videonadzora

Kontrolor koji vrši videonadzor dužan je:

- ✓donijeti odluku koja će sadržavati pravila obrade s ciljem poštivanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako videonadzor nije propisan zakonom,
- ✓na vidnom mjestu istaći obavještenje o vršenju videonadzora i kontakt putem kojeg se mogu dobiti pojedinosti o videonadzoru.

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.

VIDEO NADZOR Član. 57 ZZLP

- ✓ Snimci pohranjeni putem videonadzora na određenom prostoru na osnovu kojih se može identifikovati nosilac podataka predstavljaju zbirku ličnih podataka.
- ✓ Kontrolor koji vrši videonadzor dužan je:
- donijeti odluku koja će sadržavati pravila obrade s ciljem poštivanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako videonadzor nije propisan zakonom,
- na vidnom mjestu istaći obavještenje o vršenju videonadzora i kontakt putem kojeg se mogu dobiti pojedinosti o videonadzoru.

ŠTA NE SMIJE BITI POKRIVENO VIDEO NADZOROM

- Sanitarni čvorovi,
- Svlačionice/garderobe,
- Prostorije za odmor: čajna kuhinja ili prostorija za pušenje duvanskih proizvoda,
- „obična radna mjesta“ – kancelarijski prostor za razliku od npr. šaltera, odn. blagajne u bankama, trgovačkim centrima i sl., ulaz/izlaz u objekat, recepcija u hotelu.

UPOTREBA RAZLIČITIH TEHNOLOGIJA ZA NADZOR RADNIKA I TREĆIH LICA

- Video nadzor
- Audio nadzor
- Kontrola elektronske pošte
- Kontrola pristupa internetu
- Kontrola pristupa
- Kontrola pristupa čuvarske službe
- Kontrola radnog vremena
- GPS (skr. Globalni pozicioni sistem)

AUDIO NADZOR / PRISLUŠKIVANJE

- Nije posebno uređeno ZZLP.
- KD Neovlašćeno prisluškivanje i tonsko snimanje (čl. 155. KZRS) - Ko posebnim uređajima neovlašćeno prisluškuje ili tonski snimi razgovor ili izjavu koja mu nije namijenjena ili omogući nepozvanom licu da se upozna sa razgovorom ili izjavom koja je neovlašćeno prisluškivana ili snimana kazniće se novčanom kaznom ili kaznom zatvora do jedne godine.
- Snimanje audio-zapisa dozvoljeno je samo radi dokazivanja komercijalnih transakcija ili drugih poslovnih odnosa, npr. radi poboljšanja usluge može se snimati razgovor zaposlenog u call centru pri razgovoru sa klijentom.

Kada bi audio snimanje bilo opravdano?

- Primjer dokazivanje mobinga ako nema mogućnosti videonadzora

1. (V.N.)
2.

https://nova.rs/vesti/drustvo/zasto-vicete-na-mene-zato-sto-ste-kreten-otkrivamo-skandalozan-mobing-direktora-instituta-za-reumatologiju-prema-zaposlenima/

PRAĆENJE KRETANJA ZAPOSLENIH PUTEM GPS

ZOR ne uređuje posebno ovu oblast , nego Zakon o zaštiti na radu kroz zaštitu radnika, ali i zaštitu imovine i drugih interesa poslodavca.

Na strani poslodavca ova mjera se može obrazložiti povećanjem kvaliteta posla u kraćem vremenu i smanjenje troškova rada, što sa druge strane za radnika može predstavljati pritisak i ograničavanje kretanja, odn. psihološki mobing.

OPREMA ZA OTKRIVANJE LOKACIJE RADNIKA

Poslodavac treba da svojim aktom da propiše:

- kada i pod kojim uslovima se koristi oprema koja otkriva lokacije radnika, zbog čega se uvodi (radi zaštite proizvodnje, zdravlja i sigurnosti, zaštite poslovne tajne u procesu proizvodnje ili druge radne aktivnosti radnika, zaštite radnika na poslovnom putu i iz kojih razloga i sl.) ,
- na koji način će se koristiti i koja oprema,
- kako se obezbjeđuje garancije za prava na privatnost i zaštitu ličnih podataka tih lica, uključujući i dodatne sigurnosne mjere .

RAD NA DALJINU I KONTROLA UČINKA

- ✓ Došao u fokus za vrijeme pandemije
- ✓ od kuće mogu obavljati uglavnom kancelarijski poslovi uz obavezu radnika da u radno vrijeme bude dostupan poslodavcu putem telefona, elektronske pošte ili na drugi način.
- ✓ Kako ovdje dolazi do preplitanja privatne i poslovne sfere, poslodavac mora da vodi računa da previše ne zadire u privatni život radnika npr. video pozivi, video kamere i sl.

To znači da poslodavac nije ovlašten vršiti nadzor nad radom radnika koji radi od kuće.

Ali može vršiti nadzor rezultata rada.

Također, radnik je obavezan da poslodavcu dostavi rezultate svog rada u vremenskim periodima i način kako se radnik i poslodavac dogovore, također elektronskim putem.

RAD NA DALJINU – Zaštita podataka

- povećava se rizik „oticanja“ ili zloupotrebe određenih podataka koji su važni za poslodavca, jer imaju karakter povjerljivih podataka i zaštićeni su kao poslovna tajna ili su u pitanju LP zaštićeni zakonom.

Uobičajene mjere zaštite:

- instaliranje odgovarajuće softverske zaštite
- uvođenje antivirusnih programa
- povremene promjene lozinke
- dvojna zaštita (back-up) snimljenih podataka.

Zaštita materijalnih isprava

POSLOVNI E-MAIL

U pravilu, elektronsku poštu radnika treba nadzirati samo u izuzetnim okolnostima, npr. zbog potvrde ili dokaza njegovih kriminalnih aktivnosti, ako je to neophodno zbog odbrane interesa poslodavca u slučajevima kada on posredno odgovara za aktivnosti radnika, povreda radne dužnosti, odavanje poslovnih informacija, sumnja na mobing i sl.

Ako je radnik vanredno izostao sa posla, može biti nužno otvaranje el.pošte zbog održavanja poslovne korespondencije.

Ako se ovi podaci prikupljaju za određenu,izričitu i legitimnu svrhu oni ne smiju dalje biti obrađivani na način nespojiv sa tom svrhom.

Poslodavci treba da izbjegavaju:

- neopravdano i nerazumno uplitanje u pravo na privatni život radnika,
- neodoboreno pristupanje poslodavca profesionalnim elektronskim komunikacijama njihovih zaposlenih osim kada je neophodno za sigurnost ili iz drugih legitimnih razloga,
- ni pod kojim okolnostima ne treba da se nadzire sadržaj, slanje i primanje privatne elektronske komunikacije na poslu i slično.

BĂRBULESCU PROTIV RUMUNJSKE

tijekom nadzora utvrđeno da je podnositelj koristio Internet u osobne svrhe. Iako je podnositelj tvrdio da je Internet koristio isključivo u poslovne svrhe, suočen je s transkriptom poruka na Yahoo Messengeru iz kojih je vidljivo da je razmjenjivao poruke sa bratom i zaručnicom o privatnim stvarima poput zdravlja i seksualnog života. U kolovozu 2007. podnositelj je dobio otkaz zbog povrede internih pravila tvrtke koja zabranjuju korištenje resursa tvrtke u privatne svrhe.

OCJENA SUDA Sud je najprije ocijenio da je članak 8. Konvencije primjeniv na ovaj predmet zbog činjenice da je poslodavac pristupio podnositeljevom poslovnom računu te zbog činjenice da je zapis o njegovoj komunikaciji putem tog računa bio korišten u domaćem postupku. Međutim, Sud smatra razumnom namjeru poslodavca da provjeri izvršavaju li zaposlenici svoje poslovne obveze tijekom radnog vremena, te primjećuje da je poslodavac pristupio podnositeljevom računu vjerujući da sadrži poslovnu komunikaciju s klijentima.

OBRADA PODATAKA O ČLANOVIMA PORODICE RADNIKA

Ime i prezime, te datum rođenja djece i bračnog druga, imovinski karton te druge važne podatke.

Informacije potrebne za organizaciju različitih događaja i benefita za radnike *(npr. novogodišnji paketići, zajednički team building, davanje prednosti djeci radnika u procesima stipendiranja i organizacija školskih praksi).*

Podaci za supružnike su traženi zbog plana da se u bliskoj budućnosti organizuje „Family day“ za radnike i članove njihove porodice.

organizovanje navedenih i sličnih događaja nije regulisano zakonskom materijom kao obaveza poslodavca ili pravo radnika iz radnog odnosa, da bi se posebno prikupljali podaci o radnicima i članovima njihove porodice.

Poslodavac može vršiti obradu samo onih ličnih podataka radnika koji su od neposrednog značaja za poslove koje obavljaju ili su potrebni radi dokazivanja prava i dužnosti iz radnog odnosa.

Kada su u pitanju lični podaci članova porodice radnika, obradu istih poslodavac može vršiti samo ukoliko su potrebni radi dokazivanja prava iz radnog odnosa radnika kao što je pravo na zdravstveno osiguranje za članove porodice, poreske olakšice, određene naknade i slično.

I pored činjenice da poslodavac kroz personalnu evidenciju već obrađuje jedan dio ličnih podataka radnika koji se traži predmetnim obrascem, dodatno prikupljanje tih podataka u naprijed navedenu svrhu i njihova dalja obrada kroz posebne evidencije, programe, baze i slično, ne nalazi svoje uporište u Zakonu o radu ni drugom posebnom propisu.

Čak i kada se prikupljanje podataka vrši na osnovu saglasnosti, koju radnik daje svojim potpisom ispod popunjenog obrasca tabele sa traženim podacima smatra se da se obrada vrši na osnovu zakonskih propisa pravni osnov je sadržan u relevantnim zakonima i ne može zavisiti od volje pojedinca tj. njegove saglasnosti.

SIGURNOSNE PROVJERE ZAPOSLENIKA

- ✓ prije zaposlenja i
- ✓ periodične tijekom trajanja radnog odnosa

Pr. Osnov:

- Zakon o zaštiti tajnih podataka (SGBIH 54/2005, 12/09)
- Podzakonski akti dostupni na:

http://msb.gov.ba/Zakoni/akti/default.aspx?id=11443&langTag=bs-BA

(2) Podaci iz upitnika, koji je popunila osoba za koju se radi sigurnosna provjera, uspoređuju se s podacima iz službene evidencije kojom raspolaže OSA BiH, kao i podacima drugih nadležnih državnih organa i ostalih odgovarajućih izvora podataka utvrđenih posebnim pravilnikom, koji donosi Vijeće ministara BiH i koji je usaglašen sa Zakonom.

Osnovni upitnik

Osoba koja je predmet sigurnosne provjere popunjava sigurnosne upitnike i izjavu o upoznavanju sa propisima iz oblasti zaštite tajnih podataka.

Osnovni upitnik - segmenti

1. **Identifikacioni podaci**,
2. **Državljanstvo**,
3. **Adrese prebivališta u periodu za koji se vrši provjera**,
4. **Adrese boravišta u periodu za koji se vrši provjera**: **Boravište**
5. **Boravak u inostranstvu duži od tri mjeseca**,
6. **Bračno stanje**,
7. **Lični podaci bračnog/vanbračnog partnera i punoljetnih osoba koji sa vama žive u zajednici**,

8. Školovanje i stečena stručna sprema i zvanje,
9. Školovanje i učešće na seminarima ili drugim oblicima obrazovanja i usavršavanja u inostranstvu u periodu za koji se radi provjera, ako su trajala duže od tri mjeseca,
10. Radno-pravni status,
11. Dosadašnji poslodavci i njihove adrese,
12. Služenje vojnog roka i angažman u oružanim snagama ili drugim naoružanim formacijama,
13. Da li je protiv vas bila izrečena pravnosnažna presuda zbog krivičnih djela,
14. Da li je protiv vas bilo doneseno rješenje o prekršajima iz sadržaja Zakona o zaštiti tajnih podataka,
15. Da li se protiv vas vodi krivični postupak,

16. Da li ste ikada bili ovisnik o alkoholu, drogama ili drugim oblicima ovisnosti,
17. Da li ste ikada bili u kontaktu sa stranim sigurnosnim ili obavještajnim službama,
18. Da li ste bili član ili imali saradnju sa organizacijama ili pojedincima koji se bave kriminalom, zagovaraju terorizam ili druge protu-ustavne načine promjene ustavnog poretka BiH ili učestvuju u njihovom finansiranju,
19. Da li je protiv vas u posljednje dvije godine bila izrečena disciplinska mjera zbog kršenja propisa o obradi tajnih podataka,
20. Da li su za vas ranije vršene sigurnosne provjere u skladu sa tadašnjim zakonima ili u skladu sa Zakonu o zaštiti tajnih podataka,
21. Imovinsko stanje provjeravane osobe i imovinsko stanje bračnog ili vanbračnog partnera i punoljetnih osoba koje sa provjeravanom osobom žive u zajednici.

Druge vrste upitnika

Sadržaj sigurnosnih upitnika propisan je Zakonom.

Izgled sigurnosnih upitnika propisan je na obrascima koji su sastavni dio ovog Pravilnika i to:

a) Osnovni sigurnosni upitnik - Obrazac A,

b) Posebni sigurnosni upitnik - Obrazac B,

c) Dodatni sigurnosni upitnik - Obrazac C,

d) Dodatni sigurnosni upitnik u slučaju sigurnosne smetnje - Obrazac D.

Sastavni dio sigurnosnih upitnika je Saglasnost za provjeru koju daje provjeravana osoba, te Izjava kojom provjeravana osoba potvrđuje da je upoznata sa propisima iz oblasti zaštite tajnih podataka i obavezuje se da će sa tajnim podacima postupati u skladu sa propisima.

Obaveze kontrolora u javnom sektoru prema novom ZZLP

-
-

- **Tehničke i organizacione mjere**
- Uloga službenika za zaštitu ličnih podataka
- Sigurnosne mjere i procjena rizika
- Postupanje u slučaju povrede sigurnosti podataka

ULOGA SLUŽBENIKA 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



SIGURNOSNE MJERE I PROCJENA RIZIKA

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.

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



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:

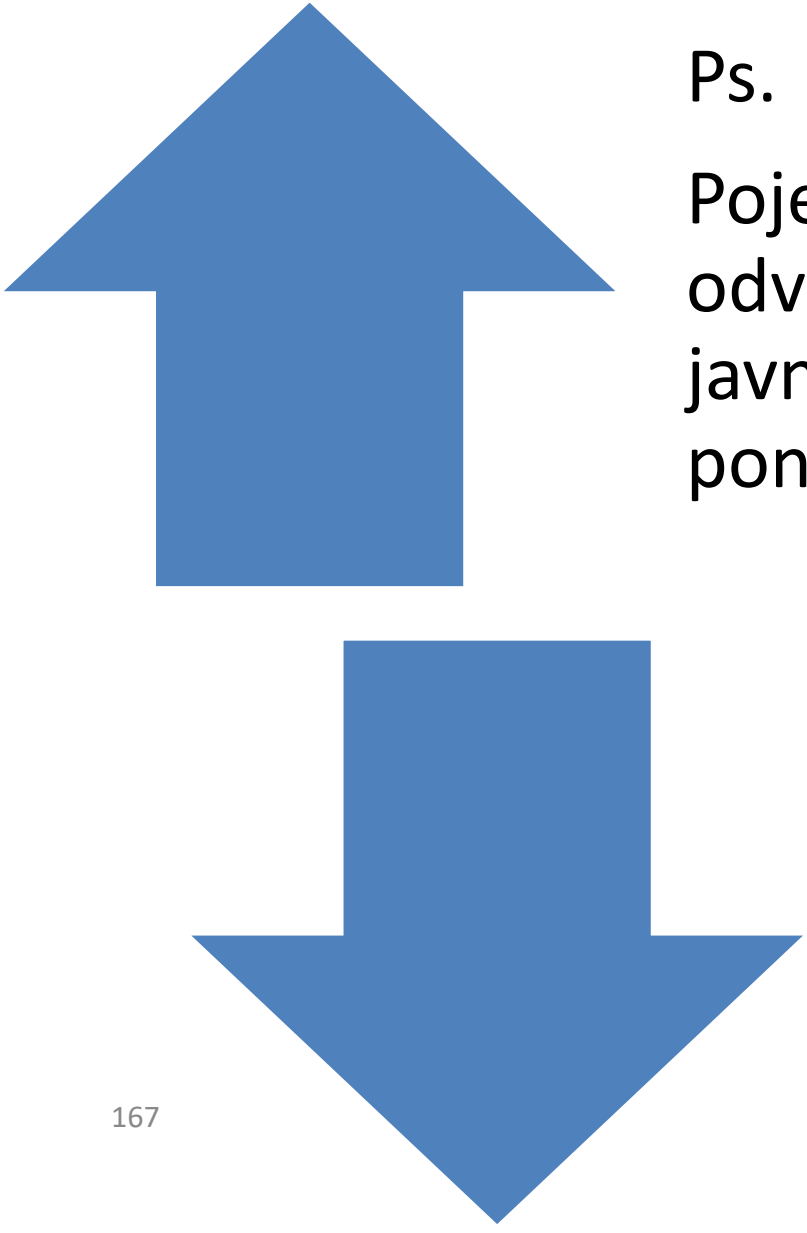
Načela zaštite podataka stoga se ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ili na osobne podatke koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi. 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.

Anonimizacija vs. pseudonimizacija



Ps.

Pojedinac se može, uz pomoć odvojeno čuvanih podataka ili javno dostupnih informacija ponovo identifikovati.

An.

Pojedinac se ne može identifikovati ili se može identifikovati samo uz ogromne napore.

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.

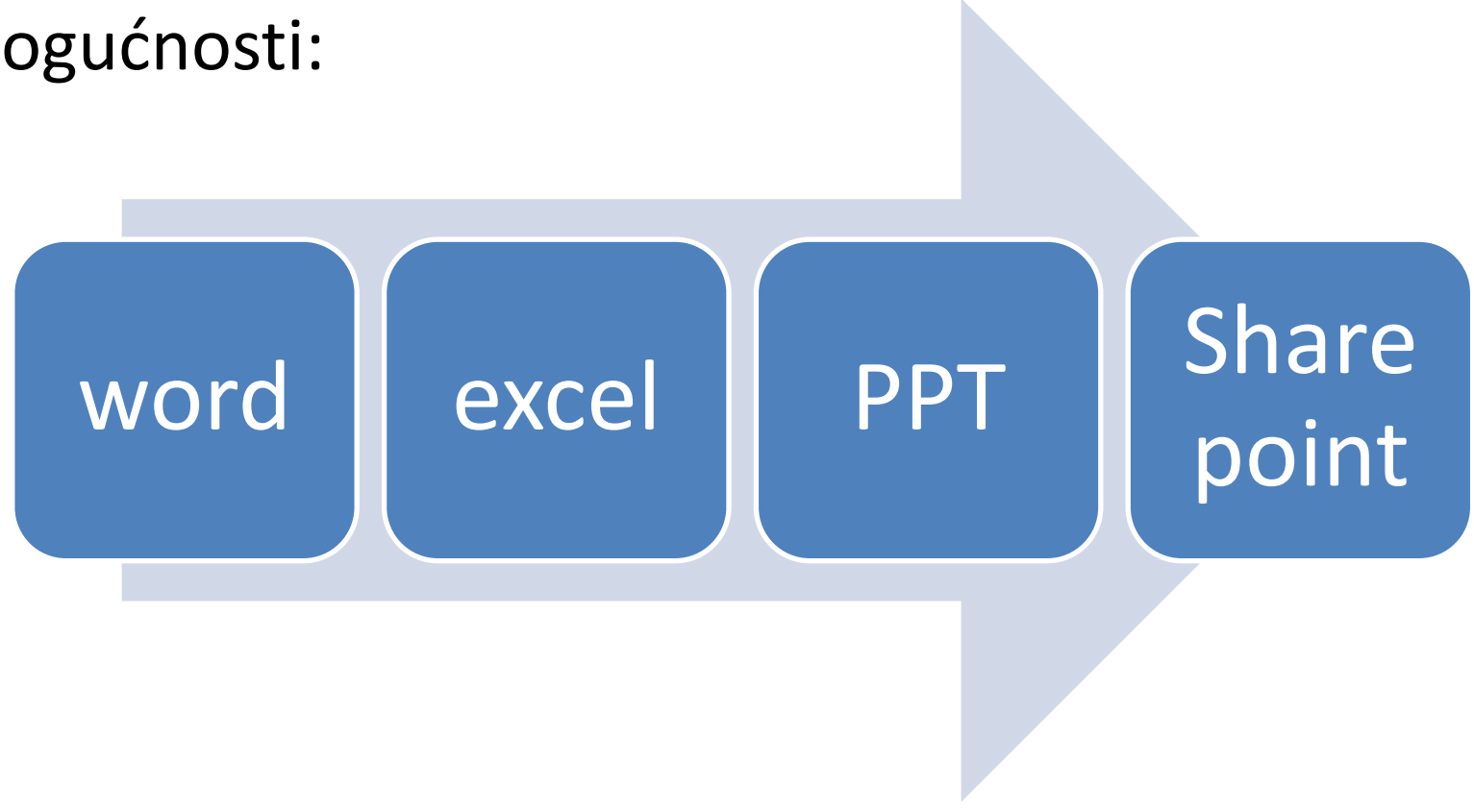
Sadržaj evidencije

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

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.

POSTUPANJE U SLUČAJU POVREDE PODATAKA

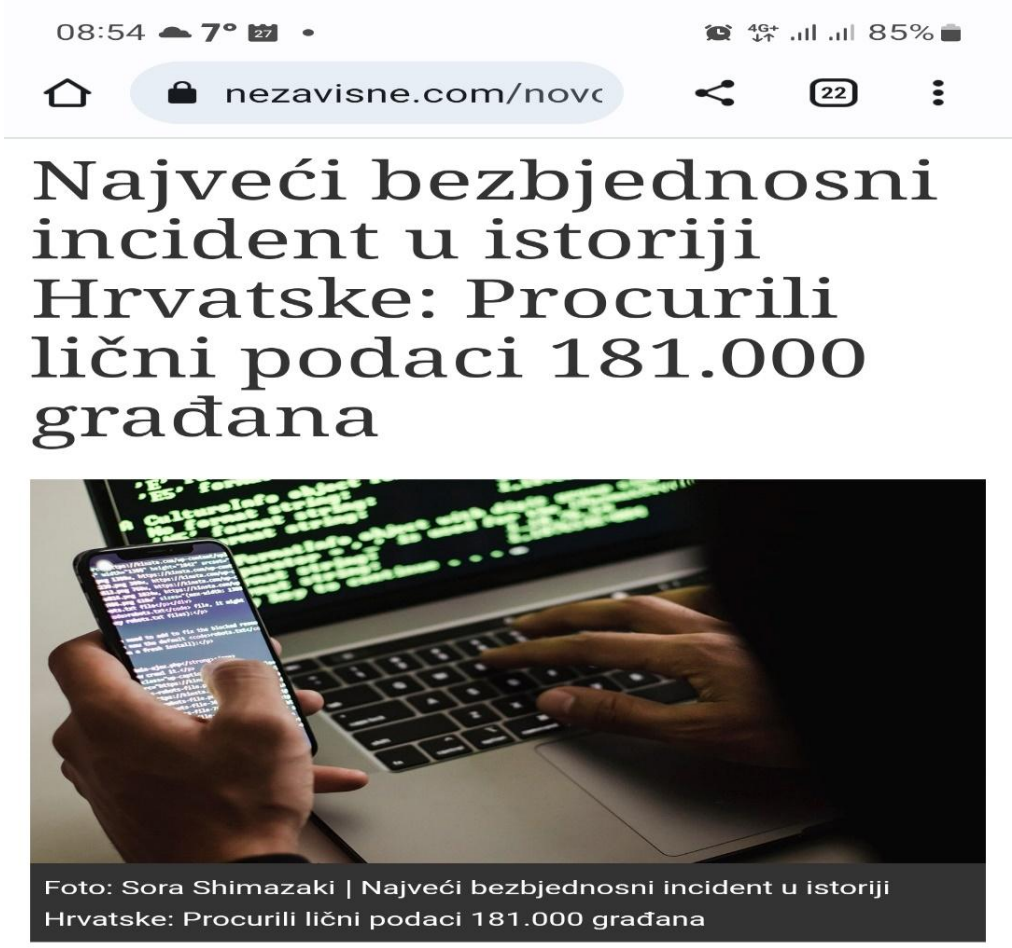
Decembar 2022.

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



Najveći bezbjednosni incident u istoriji Hrvatske: Procurili lični podaci 181.000 građana

Foto: Sora Shimazaki | Najveći bezbjednosni incident u istoriji Hrvatske: Procurili lični podaci 181.000 građana

Nezavisne novine
27.03.2023 07:45

ZAGREB - Iz kompanije EOS Matriks, koja pomaže preduzećima da profesionalno naplate dugove, procurilo je više od 181.000 ličnih podataka građana Hrvatske, a među njima su i podaci par stotina maloljetnih osoba, što je najveće curenje



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.

ZAKLJUČCI/ PREPORUKE

Naslov

Sadržaj teksta /Normal- Arial 11, poravnjanje

Naslov

Sadržaj teksta /Normal- Arial 11, poravnjanje

Naslov

Sadržaj teksta /Normal- Arial 11, poravnjanje

EFFECTIVE CAF 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