REVIZIJA ZAŠTITE LIČNIH PODATAKA

PRAKTIČAN PRIMJER

Pravni okvir u Bosni i Hercegovini

- Ustav Bosne i Hercegovine,
- Zakon o zaštiti ličnih podataka (stari zakon) (Službeni glasnik BiH broj 49/06, 76/11, 89/11),
- Zakon o zaštiti ličnih podataka (novi zakon) (Službeni glasnik BiH broj 12/25),
- Sporazum o stabilizaciji i pridruživanju između evropskih zajednica i njihovih država članica i Bosne i Hercegovine.

Međunarodni izvor prava

- Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (1950),
- Povelja Evropske unije o osnovnim pravima,
- Uredba Evropske unije 2016/679 o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka te o stavljanju van snage Direktive 95/46 Evropske zajednice – Opšta uredba o zaštiti ličnih podataka – GDPR.

Osnovni pojmovi

- Lični podaci podrazumijevaju bilo koju informaciju koja se odnosi na fizičko lice koje je identifikovano ili može da se utvrdi identitet lica.
- Zaštita ličnih podataka odnosi se na skup pravila, mjera i principa koji imaju za cilj da sačuvaju privatnost pojedinca i spriječe zloupotrebu informacija koje ga identifikuju.
- Zakonom o zaštiti ličnih podatka štite se osnovna prava i slobode fizičkih lica u Bosni i Hercegovini bez obzira na njihovo državljanstvo i prebivalište, a posebno njihovo pravo na zaštitu ličnih podataka.

Osnovni pojmovi

- Nosilac podataka – fizičko lice čiji se identitet može ustanoviti ili identifikovati, neposredno ili posredno, naročito na osnovu jedinstvenog matičnog broja te jednog ili više faktora karakterističnih za fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet tog lica.
- Obrada ličnih podataka – podrazmijeva bilo koju radnju ili skup radnji koje se vrše nad podacima, bilo da je automatska ili ne, a posebno prikupljanje, unošenje, organizovanje, pohranjivanje, prerađivanje ili izmjenu, uzimanje, konsultovanje, korištenje, otkrivanje prenosom, širenje ili na drugi način omogućavanje pristupa podacima, svrstavanje ili kombinovanje, blokiranje, brisanje ili uništavanje.
- Zbirka ličnih podataka – sistemski skup podataka koji su dostupni prema posbenim kriterijima, bilo da su centralizovani, decentralizovani ili razvrstani na funkcionalnom i geografskom osnovu ili postavljeni u skladu s posebnim kriterijima koji se odnose na lice i koji omogućavaju nesmetan pristup ličnim podacima u dosjeu.
- Kontrolor je svaki javni organ, fizičko ili pravno lice, agencija ili drugi organ koji samostalno ili zajedno sa drugim vodi, obrađuje ili utvrđuje svrhu i način obrade ličnih podataka na osnovu zakona ili propisa.

Osnovni pojmovi - primjer

Pojam	Primjer iz prakse
Nosilac podatka	Građanin koji koristi usluge snabdijevanja; npr. vlasnik domaćinstva u Ugljeviku
Kontrolor	Direkcija za javno snabdijevanje električnom energijom ERS
Zbirka podataka	Baza korisnika električne energije: ime, JMBG, adresa, broj mjernog mjesta, potrošnja
Obrada podataka	Prikupljanje podataka, očitavanje brojila, izrada računa, slanje obavijesti, arhiviranje, naplata potraživanja i dr.

Rizik - zaštita ličnih podataka

Rizik je mogućnost da se dogodi neželjen ili štetan događaj, odnosno neizvijesnost u vezi s ishodom neke aktivnosti.

Upravljanje rizikom se definiše kao cjelokupan proces utvrđivanja, procjenjivanja i praćenja rizika za ostvarene ciljeva subjekta, kao i preduzimanje potrebnih aktivnosti, posebno kroz sistem finansijskog upravljanja i kontrola u svrhu smanjenja rizika.

Upravljanje rizikom je kontinuirana aktivnost koja obuhvata utvrđivanje rizika, procjenu njihove vjerovatnoe i uticaja, preduzimanje mjera kao odgovor na rizike, dokumentovanje podataka o najznačajnijim rizicima i praćenje i izvještavanje o rizicima. To je proces koji provodi rukovodilac subjekta u cijelom subjektu sa ciljem identifikovanja potencijalnih događaja koji mogu negativno uticati na subjekt kako bi se sveli u granice prihvatljivog.

STRATEGIJE UPRAVLJANJANA RIZIKOM ZAŠTITE LIČNI PODATAK

Eliminacija aktivnosti koje nose visok rizik

Uvođenje mera koje umanjuju rizik

PRENOŠENJE RIZIKA

Prebacivanje rizika na treću stranu

PRIHVATANJE RIZIKA

Svesno preuzimanje prihvatljivog rizika

Strategija	Opis	Konkretne mjere / primjeri
Izbjegavanje rizika	Eliminacija aktivnosti koje nose visok rizik	• Ne prikupljati nepotrebne podatke (npr. JMBG bez pravne osnove). • Izbjegavanje obrade osjetljivih podataka bez jasnog opravdanja. • Ne koristiti nesigurne servise za obradu podataka.
Smanjenje rizika	Umanjenje vjerovatnoće ili posljedica rizika	• Enkripcija i pseudonimizacija podataka. • Ograničen pristup podacima. • Obuka zaposlenih. • Incident response plan.
Prenošenje rizika	Prebacivanje rizika na treće strane	• Ugovori sa obrađivačima podataka (npr. IT firme). • Cyber osiguranje. • Korištenje sertifikovanih servisa (npr. ISO 27001).
Prihvatanje rizika	Svjesno preuzimanje kontrolisanog i prihvatljivog rizika	• Privremeno čuvanje podataka u papirnom obliku. • Interni sistemi bez dodatne enkripcije za neosjetljive podatke. • Odluka da se ne ulaže u dodatne alate kada je rizik minimalan.

Globalni standardi interne revizije

Pet domena:

- Svrha interne revizije,
- Etika i profesionalizam,
- Upravljanje funkcijom interne revizije,
- Rukovođenje funkcijom interne revizije i
- Obavljanje usluga interne revizije.

Domen I Izjava o svrsi

Interna revizija jača sposobnost organizacije da stvori, zaštiti i održi vrijednost tako što pruža odboru i menadžmentu nezavisno, objektivno i na riziku zasnovano uvjeravanje savjet, uvid i predviđanje.

Interna revizija poboljšava organizaciju kroz:

- Uspješno postizanje svojih ciljeva.
- Procese upravljanja, upravljanje rizikom i kontrolu.
- Donošenje odluka i nadzor.
- Ugled i kredibilitet kod zainteresiranih strana.
- Sposobnost služenja javnom interesu.

Interna revizija je najefikasnija kada:

- Se izvodi od strane kompetentnih profesionalaca u skladu sa Globalnim standardima interne revizije,a koji su postavljeni u javnom interesu.
- Funkcija interne revizije je nezavisno pozicionirana sa direktnom odgovornošću odboru.
- Interni revizori su oslobođeni neprimjerenog utjecaja i posvećeni davanju objektivnih procjena.

Domen IV Rukovođenje funkcijom interne revizije

Domen IV obuhvata 4 principa:

- ✓Princip 9 Planiraj strateški,
- ✓Princip 10 Upravljajte resursima,
- ✓Princip 11 Komunicirajte efikasno i
- ✓Princip 12 Poboljšajte kvalitet.

Svi principi ovog domena odnose se na Glavnog izvršnog revizora što prema našim propisima je Rukovodilac interne revizije ili Direktor Odjeljenja interne revizije.

Princip 9 Planirajte strateški

Glavni Izvršni revizor strateški planira da pozicionira funkciju interne revizije da ispuni svoj mandat i postigne dugoročni uspjeh.

Standardi:

- ✓9.1 Razumijevanje upravljanja, upravljanja rizikom i procesa kontrole,
- ✓9.2 Strategija interne revizije,
- ✓9.3 Metodologije,
- ✓9.4 Plan interne revizije,
- ✓9.5 Koordinacija i oslanjanje.

Uočeni rizici u vezi sa zaštitom ličnih podataka

Rizik da nije uspostavljen dovoljan nivo internih kontrola

- ✓ Nije donijet akt o zaštiti ličnih podataka (pravilnik),
- ✓ Nije uspostavljen registar zbirki ličnih podataka,
- ✓ Postojeći interni akti nemaju ugrađene elemente zaštite ličnih podataka,
- ✓ Nisu dodijeljena ovlaštenja i odgovornosti i dr.

Rizik poštovanja internih procedura

- ✓ Nije uspostavljena kontrola nad pristupom podacima,
- ✓ Nije definisana svrha prikupljanja podataka,
- ✓ Nije imenovano lice – službenik za zaštitu ličnih podataka
- ✓ Ne poštuju se dodijeljena ovlaštenja,
- ✓ Nije uspostavljena dovoljna svijest o značaju zaštite ličnih podataka

Uočeni rizici u vezi sa zaštitom ličnih podataka

Rizik vezan za kadrovska pitanja:

- ✓Nije definisano u ugovorima o radu i opisu poslova obaveza čuvanja poslovne tajne, zaštita ličnih podataka i sl.
- ✓Nisu preduzete fizičke mjere na zaštiti ličnih podataka zaposlenih

Rizik informacionog sistema:

- ✓Nisu implementirana rješenja koja sprečavaju neovlašteni pristup, krađu podataka, gubitak podataka, curenje podataka i dr.
- ✓Dozvoljen je pristup mreži sa privatnih uređaja, korištenje privatnih naloga i sl.

Primjer rizika kod video nadzora

Kategorija rizika	Opis	Primjer
Nejasna svrha nadzora	Ako svrha nije jasno definisana, dolazi do pravne nesigurnosti.	Subjekt nije dokumentovao da je cilj zaštita imovine, već se nadzor koristi i za praćenje zaposlenih.
Nedostatak obavještenja	Zakon zahtijeva jasno istaknuto obavještenje o video nadzoru.	Kamere su postavljene bez naljepnica ili obavještenja na vidljivim mjestima.
Neovlašteni pristup snimcima	Ako snimke može pregledati bilo ko, dolazi do povrede privatnosti.	Tehničko osoblje ima pristup svim snimcima bez kontrole ili evidencije.
Prekomjerna obrada podataka	Snimanje prostora koji nije nužan za zaštitu imovine.	Kamera snima prostoriju za odmor zaposlenih, što nije opravdano.
Nedostatak odluke o obradi	Kontrolor mora donijeti formalnu odluku o obradi putem video nadzora.	Firma nije donijela internu odluku sa definisanim pravilima obrade.
Neinformisani zaposleni	Zaposleni moraju biti obaviješteni o svrsi i obimu nadzora.	Radnici nisu upoznati da se hodnici snimaju 24/7.
Predugo čuvanje snimaka	Zakonom se propisuje razuman rok čuvanja.	Snimci se čuvaju godinu dana bez opravdanja — što je prekomjerno.
Neprijavljena zbirka podataka	Video snimci koji omogućavaju identifikaciju predstavljaju zbirku.	Subjekt nije prijavio zbirku Agenciji za zaštitu ličnih podataka BiH.
Zloupotreba snimaka	Snimci se koriste u svrhe koje nisu prvobitno definisane.	Snimak se koristi za disciplinsku mjeru bez prethodne najave takve svrhe.

Primjer rizika kod evidencije o zaposlenima

Kategorija rizika	Opis	Primjer iz prakse
Neovlašteni pristup evidenciji	Zaposleni koji nemaju potrebu za pristupom podacima ipak imaju tehnički pristup.	Računovođa ima pristup dosjeima sa zdravstvenim podacima zaposlenih.
Prekomjerna obrada podataka	Prikupljaju se podaci koji nisu nužni za radni odnos.	HR traži podatke o bračnom statusu i broju djece bez jasne svrhe.
Neadekvatno čuvanje dokumentacije	Fizički dosjei se čuvaju u otvorenim ormarićima, digitalni bez lozinke.	Bilo ko može uzeti ili fotografisati podatke iz kadrovske evidencije.
Nedostatak saglasnosti za posebne podatke	Osjetljivi podaci (npr. zdravstveni, etnički) se obrađuju bez izričite saglasnosti.	Podaci o bolovanju se šalju trećim licima bez pristanka.
Neinformisani zaposleni	Zaposleni ne znaju koja se obrada vrši, ko ima pristup i koja su njihova prava.	Novi radnici nisu upoznati sa politikom privatnosti firme.
Nejasna svrha obrade	Firma ne dokumentuje zašto se određeni podaci prikupljaju.	Prikupljaju se podaci „za svaki slučaj“, bez definisane potrebe.
Neusklađenost sa rokovima čuvanja	Podaci se čuvaju duže nego što je zakonom dozvoljeno.	Dosjei bivših zaposlenih se čuvaju više od 10 godina bez pravnog osnova.
Zloupotreba podataka od strane zaposlenih	Interni podaci se koriste u privatne svrhe.	HR radnik koristi kontakt podatke zaposlenih za privatne pozive.
Nedostatak interne politike zaštite podataka	Ne postoje jasna pravila o obradi, pristupu i čuvanju podataka.	Svaki sektor vodi evidenciju na svoj način, bez kontrole.

Standard 9.4 Plan interne revizije

- **Glavni izvršni revizor mora kreirati plan interne revizije koji podržava postizanje ciljeva organizacije.**
- Plan mora zasnovati na dokumentovanoj procjeni strategija, ciljeva i rizika organizacije baziranoj na inputima od odbora i višeg menadžementa, kao i na razumijevanju glavnog izvršnog revizora o upravljanju organizacijom, upravljanju rizicima i procesima kontrole.
- Procjena mora biti obavljena najmanje jednom godišnje.
- Glavni izvršni revizor mora pregledati i revidirati plan interne revizije po potrebi i blagovremeno obavijestiti odbor i viši menadžment.
- Plan i značajne izmjene plana mora odobriti odbor.

Standard 9.4 Plan interne revizije

Plan interne revizije treba da sadrži:

- Resurse i dostupne sate za angažmane (revizije, administrativni poslovi, nerevizijske aktivnosti i dr.)
- Spisak predloženih angažmana,
- Obrazloženje za odabir svakog predloženog angažmana (rizik, regulatorni zahtjev, proteklo vrijeme od prethodnog angažmana, trend, organizacija i sl.)
- Opšta svrha i preliminarni obim svakog predloženog angažmana,
- Procenat sati za nepredviđene slučajeve, ad hoc zahtjeve i dr. Elemente.

Naziv revizije	Revizija zaštite ličnih podataka
Planirani period sprovođenja	Mart i april 2025. godine
Planirano vrijeme	60 revizorskih dana
Revizori	Kristina Milivojević, Jelena Krsmanović i NN
Potrebno angažovanje drugih lica	Angažovati u fazi prikupljanja podataka i fazi testiranja programskih rješenja inženjera koji ima odgovarajuće IT znanje
Cilj revizije	Dati objektivno i nezavisno mišljenje u vezi sa efikasnošću, ekonomičnosti i efektivnosti procesa zaštite ličnih podataka kao i o usklađenosti sa zakonskih i drugim podzakonskim i internim aktima.
Obim revizije	- Preispitati da li je uspostavljen dovoljan sistem internih kontrola, - Preispitati poštovanje zakonskih i internih akata, - Testirati interne kontrole, - Dati prijedloge i preporuke u skladu sa nalazom.

Domen V Obavljanje usluga interne revizije

- Obavljanje usluga interne revizije zahtijeva od internih revizora:

➢ da efektivno planiraju angažmane,

➢ provode angažman kako bi razvili nalaze i zaključke,

➢ Sarađuju sa menadžmentom kako bi identifikovali preporuke i/ili akcione planove koji se bave nalazima i

➢ Komuniciraju s menadžmentom i zaposlenima odgovornim za aktivnosti koja se revidira tokom cijelog angažmana i nakon njegovog zatvaranja

Principi i standardi domena V

OBAVLJANJE USLUGA INTERNE REVIZIJE		
Efikasno planirajte angažmane	**Provedite rad na angažmanu**	**Saopštavajte**
13.1 Komunikacija tokom angažmana 13.2 Procjena rizika angažmana 13.3 Ciljevi i obim angažmana 13.4 Kriterijumi za evaluaciju 13.5. Resursi angažmana 13.6 Program rada	14.1 Prikupljanje informacija za analize i evaluaciju 14.2 Analize i potencijalni nalazi angažmana 14.3 Evaluacija nalaza 14.4 Preporuke i akcioni planovi 14.5 Zaključci o angažmanu 14.6 Dokumentacija o angažmanu	15.1 Konačna komunikacija o angažmanu 15.2 Potvrđivanje implementacije preporuka ili akcionih planova

Princip 13 Efikasno planirajte angažmane

Interni revizori planiraju svaki angažman koristeći sistematski, disciplinarni pristup.

Globalni standardi interne revizije i metodologija koju je uspostavio Glavni izvršni revizor čine osnovu sistematskog, disciplinarnog pristupa internih revizora.

Interni revizori su odgovorni za efikasnu komunikaciju u svim fazama angažmana.

Neophodno je razumijevanje početnih očekivanja od angažmana i razloga zašto je angažman uključen u plan interne revizije.

Rezultat ove faze je radni program angažmana koji opisuje konkretne korake angažmana koje treba izvršiti.

Standard 13.6 Program rada(primjer)

Broj revizije	3	Naziv revizije				Zaštita ličnih podataka		
Faza revizije	Aktivnosti	Revizor	Nadzor	Procijenjeni dani revizora	Rok izvođenja	Otvorena pitanja	Napomena	Referenca na dokumentaciju
Planiranje revizije	1. Utvrditi obim revizije 2. definisati cilj revizije 3. Izvršiti preliminarnu analizu rizika 4. definisati kontrolne ciljeve	Kristina Milivojević	Mile Balotić	5	10.3.2025. godine	Da li treba tražiti produženje okvirnog perioda za okončanje revizije		Dokumenta 3.1.-3.12
Utvrđivanje i dokumentovanje sistema	1. Normativna regulativa 2. Opis procesa 3. Dijagram toka	Kristina Milivojević Jelena Krsmanović	Mile Balotić	10	10.3.2025. godine			
Procjena sistema internih kontrola		Jelena Krsmanović	Kristina Milivojević	10	20.3.2025. godine			
Testiranje kontrola	1. Na osnovu definisanih kontrola izvršiti uvid da li su iste implemnetirane	Jelena Krsmanović	Kristina Milivojević	26	10.4.2025. godine			
Konačna ocjena sistema internih kontrola		Kristina Milivojević	Mile Balotić	3	17.4.2025. godine			
Nacrt revizorskog izvještaja	1. Izrada nacrta revizorskog izvještaja 2. usaglašavanje izvještaja sa Direktorom OIR 3. Završni sastanak	Kristina Milivojević	Mile Balotić	4	20.4.2025. godine			
Konačan izvještaj	1. Izvršiti eventualne korekcije nakon usaglašavanja izvještaja sa revidovanim subjektom	Kristina Milivojević	Mile Balotić	2	30.4.2025. godine			

Princip 14 Provedite rad na angažovanju

Interni revizori implementiraju program rada angažmana kako bi postigli ciljeve angažmana.

Za implementaciju radnog programa angažmana, interni revizori prikupljaju informacije i vrše analize i evaluacije kako bi izradili dokaze.

Ovi koraci omogućavaju internim revizorima da:

- Daju sigurnost i identifikuju potencijalne nalaze,
- Utvrde uzroke, posljedice i značaj nalaza,
- Razviju preporuke i/ili sarađuju sa menadžmentom na izradi akcionih planova i
- Izrađuju zaključke.

Test kontrole – video nadzor

Kontrole	Nalaz
Da li je donijeta odluka o uvođenju video nadzora?	Nije donijeta odluka
Da li je u odluci navedena svrha, šta su potencijalni problemi, šta su prednosti odnosno koristi koje se očekuju od uvedenog sistema?	Nije donijeta odluka
Ko je bio predlagač odluke?	Služba obezbjeđenja je bila predlagač odluke o nabavci sistema video nadzora
Ko je zadužen za nabavku, izradu projekta, čije je vlasništvo?	Nabavku sprovele stručne službe, izrada projekta je bila interna, ali nakon ulaska dobavljača u realizaciju ugovora, došlo je do izmjene projetka tj činjenično stanje je drugačije i razlikuje se od projekta, interno izrađeni projekat nije dorađen. Nije poznato koje područje je obuhvaćeno svakom kamerom.
Da li je prikupljena saglasnost zaposlenih za snimanje?	Nije
Da li su na vidnom mjestu istaknuta obavještenje o snimanju?	Nisu
Da li postoji interni akt kojim su definisane dužnosti i obaveze zaposlenih u vezi sa video nadzorom?	Ne
Da li je definisano ko ima pristup da gleda uživo?	Ne, svi zaposleni iz obezbjeđenja, IT službe imaju pristup i mogu da prate uživo
Da li je definisano gdje se čuvaju snimci i koliko dugo?	Nije definisano, po potrebi
Da li je definisano ko je vlasnik opreme?	Vlasnik je IT, što prema mišljenju interne revizije nije ispravno vlasnik treba da bude služba obezbjeđenja.
Da li je definisano ko je zadužen za servisiranje i održavanje opreme?	Nije definisano, najčešće to rade zaposleni iz IT službe.

Test kontrole – evidencije o kadrovima

Kontrole	Nalaz
Da li postoji interni akti kojim je regulisana zaštita ličnih podataka?	Ne
Da li postoji procedura kojim je regulisano prikupljanje podataka o zaposlenima?	Nije zvanično propisana dokumentacija koja se prikuplja prilikom zaključenja ugovora o radu, ali postoji spisak koji se uruči licu koje treba da stupi u radni odnos.
Da li se u radnom dosijeu radnika čuvaju lični podaci zaposlenih?	Da u radnom dosijeu odložen je rodni list, uvjerenje o državljanstvu, ovjerena kopija lične karte, rodni list djece, izvještaj o ljekarskom pregledu i sl.
Da li je utvrđena svrha zašto se čuvaju određena dokumenta?	Nije utvrđena svrha, npr rodni list djece se čuva u dosijeu jer prema Kolektivnom ugovoru zaposleni ima pravo na 2 dana godišnjeg odmora za dijete starosti do 7 godina i dijete ima pravo na poklon za Novu godinu, svrha u vidu neke izjave ne postoji. Podaci su pohranjeni u programu.
Da li su radni dosije radnika na bezbednom mjestu?	Radni dosijei zaposlenih se čuvaju u metalnim ormarima, međutim kako su stari dio ormara se ne može zaključati, praksa je da se ne vrši zaključavanje ormara, nego kancelarije, ključ od kancelarije može da uzme bilo ko od zaposlenihu kadrovskoj službi
Da li su bezbedni podaci pohranjeni u programu Kadrovska evidencija?	Šifru za pristup i izmjenu podataka imaju zaposleni u Kadrovskoj službi, ali i zaosleni u IT službi koji rade na razvoju aplikacije, zaposleni znaju šifre jedni od drugih, šifre su jednostavne, brojevi u nizu ili datum rođenja i sl. Ne praktikuje se promjena šifri po isteku nekog perioda. Pojedini zaposleni čak imaju napisanu šifru u rokovniku na stolu ili na cjedulji kod tastature. Program je na serveru, pristup serveru je ograničen na zaposlene u IT-u, backup podataka se ne vrši. U preduzeću se koriste standardne mjere za zaštitu od upada, kao što su antivirusi, ne postoji veliki stepen zaštite.

PRIMJERI IZ AGENCIJE

- Video nadzor na privatnom objektu koji snima javni put i kuće u komšiluku,
- Broj telefona u vlasništvu poslodavca,
- Objava ličnih podataka u imovinskom kartonu sa navođenjem imene djeteta i imovine djeteta,
- Provjera diploma zaposlenih,
- Zadržavanje kopije ugovora radi potvrde promjene vlasništva.

Pravna i ekonomska izdanja
za uspješno i zakonito poslovanje

BUDITE NA PRAVNOJ STRANI

www.paragraf.ba - www.paragraf.rs

HVALA NA PAŽNJI
DRAGE KOLEGE!

Kristina Milivojević

vukovickristina@gmail.com