Integracija zaštite ličnih podataka u sistem FUK

Lejla Šipur 21. i 22. 05.2026. godine

Sadržaj

- Faze usklađivanja i cheklist za zaštitu podataka
- Poslovni procesi koji obrađuju lične podatke
- Vježba Mapa poslovnog procesa
- Ključni rizici i povezivanje sa ZZLP
- Vježba registar rizika

Prepoznavanje aktivnosti obrade ličnih podataka unutar poslovnih procesa

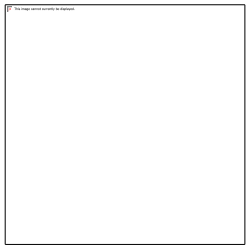
21.05.2026. godine

Faze usklađivanja

CHEKLIST
Blok 1 – Upravljanje i dokumentacija

1. Da li je rukovodstvo usvojilo akte koji uređuju zaštitu ličnih podataka (Kodeks ponašanja, Politika privatnosti, Politika kolačića)?

2. Da li su akti dostupni zaposlenicima i objavljeni na web stranici (transparentnost)?

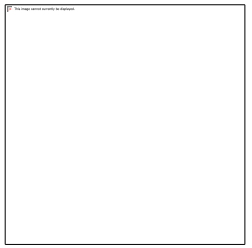


3. Da li postoji imenovani službenik za zaštitu ličnih podataka (DPO) i odluka o imenovanju u skladu sa čl. 39–41 Zakona?

4. Da li su definisane uloge i odgovornosti rukovodilaca i zaposlenika u pogledu zaštite ličnih podataka?

5. Da li je rukovodstvo upoznato sa obavezama iz Zakona o zaštiti ličnih podataka i uključeno u proces usklađivanja?

CHECKLIST
Blok 2 – Obuka



6. Da li su zaposleni upoznati s kodeksom i politikama (npr. putem edukacija ili obavještenja)?

7. Da li postoji evidencija o sprovedenim edukacijama iz oblasti zaštite ličnih podataka?

CHECKLIST
Blok 3 – Procjena rizika

8. Da li su identifikovani svi procesi koji uključuju obradu ličnih podataka?

9. Da li su prepoznati rizici po prava i slobode nosilaca podataka (npr. neovlašten pristup, gubitak podataka, neusklađena obrada)?

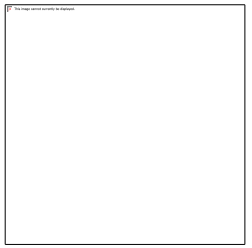
10. Da li su dokumentovani svi rizici u okviru evidencije FUK?

11. Da li se vrši procjena vjerovatnoće i uticaja svakog identifikovanog rizika?

12. Da li je izrađena Procjena uticaja na zaštitu podataka (DPIA) za visokorizične obrade (čl. 37 Zakona)?

13. Da li su definisane tehničke, organizacione i kadrovske mjere za smanjenje rizika?

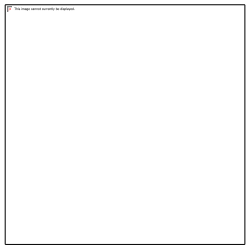
14. Da li postoji osoba odgovorna za praćenje provedbe mjera (DPO, IT, HR)?



CHECKLIST
Blok 4 – Praćenje i kontrola

15. Da li rukovodstvo redovno razmatra izvještaje službenika za zaštitu podataka i poduzima korektivne mjere?

16. Da li su obezbijeđene tehničke i organizacione mjere zaštite podataka u skladu sa članom 26. i 27. Zakona?



17. Da li se vodi evidencija aktivnosti obrade (čl. 32 Zakona)?

18. Da li su definisani postupci za prijavu i evidentiranje povreda ličnih podataka (čl. 35–36)?

19. Da li postoji postupak za prijavu i evidentiranje povreda ličnih podataka?

Kako biste se uskladili sa Zakonom o zaštiti ličnih podataka neophodno je:

- **Educirati zaposlenike** za sigurnu obradu i zaštitu podataka,
- **Uspostaviti interne procese i dokumentaciju** za evidenciju i reagovanje na povrede podataka,
- **Pratiti propise** i redovno ažurirati politiku zaštite podataka.

Najvažnije novine u odnosu na prethodni zakon:

- Šira prava građana (brisanje, prenosivost, ograničenje obrade, prigovor)
- Privatnost po dizajnu i po defaultu
- Obavezne evidencije obrade i DPIA procjene rizika
- Uvođenje DPO-a (službenika za zaštitu podataka)
- Obavezna prijava povrede podataka u roku od 72 sata
- Strožija pravila za prenos podataka u inostranstvo
- Obaveza predstavnika stranih kompanija u BiH
- Znatno veće kazne i jače ovlasti Agencije
- Posebna zaštita djece i osjetljivih podataka (16+ saglasnost)

Zakon o zaštiti ličnih podataka

„Lični podatak“je svaki podatak koji se odnosi na fizičko lice čiji je identitet utvrđen ili se može utvrditi (ime i prezime, adresa stanovanja, datum rođenja, JMBG, broj lične karte).

Podaci o zaposlenju i obrazovanju (radna biografija-CV, diplome, certifikati, ocjene),

Finansijski podaci (broj bankovnog računa, podaci sa kreditnih kartica, poreski identifikacioni broj,...),

Snimci na kojima se može identifikovati osoba (audio, video i fotografije).

Elektronski identifikatori (IP adresa/ako se može povezati sa osobom/,kolačići/ cookies/),

Zakon o zaštiti ličnih podataka

Zabranjena je obrada posebne kategorije ličnih podataka: rasno ili etničko porijeklo, političko mišljenje, vjerska ili filozofska uvjerenja, pripadnost sindikatu, genetski podaci, biometrijski podaci u svrhu jedinstvene identifikacije lica, podaci o zdravlju, polnom životu i seksualnoj orijentaciji. •

Izuzeci: Izričita saglasnost, ostvarivanje posebnih prava u oblasti radnog prava..., ostvarivanje ili odbrana od pravnih zahtjeva

- Zaštita ključnih interesa nosioca ili drugog fizičkog lica....
- Legitimne aktivnosti fondacija, udruženja
- Nosilac podataka je sam objavio podatke
- Za potrebe preventivne medicine ili medicine rada...javni interes u oblasti javnog zdravlja

COSO OKVIR

Kontrolno okruženje – Integritet i etičke vrijednosti	• Poštivanje etičkih standarda u obradi ličnih podataka, odgovornost zaposlenih za povjerljivost i zakonitu obradu podataka, sprječavanje sukobe interesa i zloupotrebe podataka.
Kontrolno okruženje – Upravljanje ljudskim resursima	• Zaposlenici imaju potrebne kompetencije i obuke za pravilnu obradu ličnih podataka.
Kontrolno okruženje – Organizaciona struktura i odgovornosti	• Jasno definisana nadležnosti i odgovornosti, uključujući imenovanje službenika za zaštitu podataka (DPO), te osiguranje da pristup podacima bude kontrolisan i odgovoran.
Kontrolno okruženje – Planiranje, misija i ciljevi	• Integracija zahtjeva za zaštitu ličnih podataka u procese organizacije.

Koji nivo zrelosti upravljanja procesima najbolje opisuje vašu organizaciju i zašto?

Organizacije sa zrelim vještinama za upravljanje svojim procesima

5. Optimizirane

Kontinuirano poboljšanje procesa osigurano kvantitativnom i kvalitativnom povratnom vezom kontrola, s pilot inovacijama i primjenom novih tehnologija.

Organizacije na ovom nivou rutinski očekuju od rukovodilaca i zaposlenih da zajedno rade na poboljšanju poslovnih procesa. Oni dovoljno dobro razumiju svoje procese da mogu sprovesti sistemske eksperimente da bi ocijenili da li će promjene biti korisne ili ne /kako za samu organizaciju, tako i za korisnike/

4. Upravljane

Detaljna mjerila kvalitete procesa i ishoda su prikupljena. I procesi i ishodi se razumiju i kontrolišu.

Nekolicina organizacija ima na nivou organizacije potpuno razumijevanje kako se procesi odnose i imaju strategiju upravljanja procesima, ciljevima i ishodima kroz organizacijsku hijerarhiju.

3. Definisane

Procesi su većim dijelom dokumentovani, standardizovani i integrisani u organizaciji

Većina organizacija je između nivoa 2. i nivoa 3. One imaju dokumentovane i standardizovane procese ali su u većini slučajeva konačni ishodi slabo povezani sa procesnim ciljevima. Indikatori mjerenja se ne prate.

2. Ponavljajuće

Zasnivanje osnovnih projekata procesnog pristupa radi određivanja troškova, slijeda aktivnosti i funkcionalnosti. Najnužnije kontrole su definisane.

Kako organizacija postaje zrelija, počinju se konceptualizirati poslovni procesi i tražiti njihova organizacija, ponavljanje uspjeha i mjerenje rezultata

1. Inicijalne

Procesi su ad hoc. Nekoliko aktivnosti je eksplicitno definisano i uspjeh ovisi o ličnim naporima i entuzijazmu učesnika.

Pojedinci u organizaciji ili neki organizacioni dijelovi čine pomake iako ne mogu započeti sa procesnim inovacijama

Organizacije sa nezrelim procesnim vještinama

Kako odrediti da li je nešto proces ili podproces?

Ako ne naljuti bar troje ljudi, onda nije riječ o procesu. Michael Hammer

Proces = šira poslovna cjelina
Podproces = dio procesa koji obuhvata srodne aktivnosti

Prilikom definisanja poslovnih procesa i podprocesa potrebno je imati u vidu:

- uspostavljenu organizacionu strukturu korisnika javnih sredstava,
- vrstu i veličinu poslovnih funkcija,
- iznos budžeta odnosno finansijskog plana,
- izvore finansiranja,
- broj zaposlenih.

Mape procesa

FUK kaže "moraš imati kontrole". Zaštita podataka kaže "kako te kontrole izgledaju kad su u pitanju lični podaci ".

Član 3. stav 1. Zakona o finansijskom upravljanju i kontroli :„Sistemom FUK obezbjeđuje se da se poslovanje javnog sektora obavlja na zakonit, efikasan, djelotvoran i transparentan način.“

Pitanje: Gdje se u FUK sistemu Vaše organizacije nalazi zaštita ličnih podataka? Da li je uopšte tu? Je li obavljena edukacija zaposlenika? Je li prepoznata zaštita ličnih podataka u kontrolnom okruženju?

Mape procesa

Naziv organizacije:	
Organizaciona jedinica:	
Rukovodilac organizacione jedinice:	

1. NAZIV PROCESA
2. CILJ PROCESA
3. OPIS ULAZNIH VRIJEDNOSTI
4. AKTIVNOSTI GLAVNE KONTROLE
5. OPIS IZLAZNIH VRIJEDNOSTI
6. RESURSI/SREDSTVA
7. ZAKONI, PODZAKONSKI AKTI I PROCEDURE KOJE SE ODNOSE NA POSLOVNI PROCES
8. ODGOVORNA LICA
9. ORGANIZACIONA JEDINICA (VLASNIK PROCESA)
10. POVEZANI POSLOVNI PROCESI

Datum:
Mjesto:

Rukovodilac organizacione jedinice

Priručnik za finansijsko upravljanje i kontrolu u javnom sektoru u Federaciji BiH("Službene novine Federacije BiH", broj: 46/23)

Mape procesa

Polje	Pitanja za popunjavanje
1. Naziv	„Šta je krajnji rezultat?“ „Kako se zove zvanični skup koraka koji transformiše ulaze u izlaze?“.....
2. Cilj	„Zašto postoji ovaj proces? Šta želimo postići?“
3. Inputi	„Šta vam je potrebno da biste pokrenuli ovaj proces? Koji dokumenti, podaci?“
4. Aktivnosti kontrole	„Koje radnje obezbjeđuju kontrolu? Šta radite prvo, pa onda?“
5. Outputi	„Šta izlazi iz ovog procesa? Koji su rezultati?“
6. Resursi	„Koje ljude, novac, opremu koristite?“
7. Zakoni	„Koji zakoni se primjenjuju?
8. Odgovorna lica	„Ko je odgovoran?“
9. Vlasnik procesa	„Koja organizaciona jedinica je zadužena da ovaj proces živi i ažurira?“
10. Povezani procesi	„Sa kojim drugim procesima je ovaj povezan?“

Mape procesa

Gdje su lični podaci u vašim procesima?

Primjeri procesa/aktivnosti koji NUŽNO obrađuju lične podatke:

- Upravljanje ljudskim resursima
- Obračun i isplata plata
- Putni nalozi
- Računovodstvo (JMBG, IBAN na računima)
- Transferi fizičkim licima
- Upravni postupak za fizička lica
- Video nadzor
- IT sistem
- .....

Mape procesa

Aktivnosti glavne kontrole???

Za svaku fazu postavlja se pitanje– koja radnja obezbjeđuje KONTROLU?

Svaki korak u procesu koji sprečava grešku, nezakonitost ili nepravilnost – jeste kontrolna aktivnost.

Mape procesa

Revizori i kontrole

Mape procesa

NAZIV PROCESA Upravljanje životnim ciklusom IT sistema

CILJ PROCESA Osigurati planiranje, razvoj, implementaciju, održavanje i povlačenje IT sistema na kontrolisan, siguran i usklađen način, uz zaštitu podataka i efikasno upravljanje resursima.

OPIS ULAZNIH VRIJEDNOSTI

- Zahtjevi korisnika (obrazac x)
- Tehničke i sigurnosne specifikacije
- Budžet/Finansijski plan
- Plan nabavke
- Postojeća IT dokumentacija i inventar

Mape procesa

KLJUČNE AKTIVNOSTI

- Analiza i odobrenje zahtjeva
- Dizajn i razvoj/nabavka sistema
- **Procjena rizika i DPIA (gdje je potrebno)**
- Implementacija sigurnosnih kontrola (MFA, enkripcija, pristupi)
- Testiranje i validacija
- Održavanje i monitoring (logovi, backup)
- Sigurno povlačenje i brisanje podataka

KONTROLE

- Odobrenje IT i rukovodstva
- Mišljenje DPO i DPIA za visokorizične obrade
- Kontrola pristupa (RBAC, MFA)
- Evidencija imovine i konfiguracija
- Logovanje i redovni pregledi
- Ugovori sa obrađivačima (DPA)
- Sigurno brisanje podataka

Mape procesa

OPIS IZLAZNIH VRIJEDNOSTI

- Funkcionalan i siguran IT sistem
- Evidencije o obradi i logovi
- Ažurirana IT inventura
- Zaštićeni i usklađeni podaci

RESURSI / SREDSTVA

- Oprema (hardver): serveri, računari, mrežna oprema, diskovi, backup uređaji IT infrastruktura i softver
- Ljudski resursi (IT osoblje, DPO, rukovodstvo)
- Finansijska sredstva
- Obuke i alati za zaštitu podataka

Mape procesa

1. NAZIV PROCESA
Upravljanje ljudskim resursima

2. CILJ PROCESA
Uspostaviti sistem ULJR koji omogućava efektivno i efikasno ispunjenje nadležnosti i ciljeva organizacije, uz poštovanje zakonskih okvira uključujući zaštitu ličnih podataka.

3. OPIS ULAZNIH VRIJEDNOSTI
• Strategija i godišnji planovi rada • Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mjesta • Budžet (sa namjenskim sredstvima za ULJR) • Zahtjevi rukovodilaca za popunjavanjem radnih mjesta • Prijave kandidata na javni oglas (lični podaci) • Zahtjevi za obukom od strane zaposlenih i rukovodilaca • Dokumentacija od zaposlenog • Evidencije

Mape procesa

4. AKTIVNOSTI GLAVNE KONTROLE
• Autorizacija • Razdvajanje dužnosti • Prethodna kontrola budžeta • Dvostruki potpis • Odobrenje • Provjera usklađenosti • Ograničenje pristupa • Provjera kompletnosti • Brisanje podataka • Provjera odstupanja

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI

- Ažuriran Pravilnik o sistematizaciji i usvojen Godišnji plan ULJR.
- Popunjena radna mjesta sa odgovarajućim kompetencijama (uz zakonitu obradu ličnih podataka).
- Realizovan plan obuka, vođen Registar obuka i sačinjen godišnji Izvještaj o obukama.
- Sprovedeno ocjenjivanje zaposlenih i sačinjen godišnji Izvještaj o upravljanju učinkom.
- Evidencija i izvještaji

6. RESURSI/SREDSTVA

- **Ljudski:** Službenik za ULJR, komisije za zapošljavanje, rukovodioci organizacionih jedinica, rukovodilac.
- **Finansijski:** Budžetska sredstva (namjenska stavka za obuke i razvoj).
- **Tehnički:** IT podrška (registar obuka, evidencije),
- **Prostor:** Za obuke, rad komisije, siguran prostor za arhiviranje (lični podaci).

Mape procesa

1. NAZIV PODPROCESA
PLANIRANJE LJUDSKIH RESURSA

2. CILJ PROCESA
Osigurati godišnje planiranje ljudskih resursa koji omogućava efektivno izvršavanje nadležnosti i strateških ciljeva organizacije, uz racionalno korištenje budžetskih sredstava.

3. OPIS ULAZNIH VRIJEDNOSTI
• Strategija razvoja • Godišnji program rada • Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mjesta • **Podaci o postojećim kadrovima (starosna struktura, kvalifikacije, fluktuacija)** • Budžet • Zahtjevi rukovodilaca organizacionih jedinica

Mape procesa

Aktivnost: Analiza postojećeg stanja ljudskih resursa (struktura, potrebe, viškovi), zahtjeva rukovodioca

Kontrola: Autorizacija analize od strane rukovodioca OJ;

Aktivnost: Godišnja analiza Pravilnika o sistematizaciji radnih mjesta (usaglašavanje sa nadležnostima)

Kontrola: Autorizacija analize od strane rukovodioca OJ;

Aktivnost: Izrada i dostavljanje plana na usvajanje

Kontrola: Provjera raspoloživosti sredstava i kompletnosti dokumentacije i dvostruki potpis na planu.

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI
• Ažuriran i usvojen Pravilnik o unutrašnjoj organizaciji i sistematizaciji radnih mjesta • Usvojen godišnji plan ULJR (sa rokovima i odgovornim licima)

6. RESURSI/SREDSTVA
• Ljudski resursi (Službenik za ULJR, Rukovodioci organizacionih jedinica) • Budžet • IT podrška (evidencije)

Mape procesa

1. NAZIV PODPROCESA
Zapošljavanje (prijem u radni odnos)

2. CILJ PROCESA
Popunjavanje upražnjenih radnih mjesta, osobama sa potrebnim kvalifikacijama i kompetencijama, kroz zakonit, transparentan i fer postupak, **uz punu zaštitu ličnih podataka kandidata**.

3. OPIS ULAZNIH VRIJEDNOSTI
. Godišnji plan ULJR (odobreni plan zapošljavanja) . Zahtjev rukovodioca za popunjavanjem radnog mjesta . Opis poslova i uslovi za radno mjesto (iz sistematizacije)

Mape procesa

Da li je sve tu?

Aktivnost: Formiranje komisije za zapošljavanje

Kontrola: Odobravanje/potpisivanje rješenja

Aktivnost: Sastavljanje teksta konkursa/oglasa i obavještenja o privatnosti za kandidate.

Kontrola: Provjera usklađenosti konkursa/oglasa i Obavještenja o privatnosti sa propisima o zaštiti ličnih podataka i internim procedurama.

Aktivnost: Prijem i evidentiranje prijava

Kontrola: Kontrola potpunosti prijave (kontrolna lista); ograničenje pristupa (zaštita ličnih podataka).

Aktivnost: Provođenje aktivnosti prijema, obrada ličnih podataka kandidata i sačinjavanje prijedloga za izbor

Kontrola: Dvostruka provjera, dokumentovanje bodovanja (revizijski trag) potpisivanje zapisnika od strane svih članova

Aktivnost: Odluka o prijemu

Kontrola: Provjera da li je odluka zasnovana na rang listi; potpis ovlaštenog lica.

Aktivnost: Prijem žalbi i provođenje žalbenog postupka

Kontrola: Čuvanje žalbene dokumentacije sa propisanim rokom

Aktivnost: Zasnivanje radnog odnosa (ugovor, rješenje)

Kontrola: Provjera usklađenosti ugovora, rješenja

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI
. Odluka o prijemu u radni odnos . Potpisan ugovor o radu/rješenje

6. RESURSI/SREDSTVA
. Ljudski resursi (Službenik za ULJR, Rukovodioc, komisija) . IT podrška (evidencije) . Prostorija za intervjue

Mape procesa

1. NAZIV PODPROCESA
Obuka i razvoj zaposlenih

2. CILJ PROCESA
Jačati kompetencije zaposlenih kroz sistematsku, planiranu i evaluiranu obuku, kako bi se efikasno i efektivno ispunjavale nadležnosti i ciljevi organizacije.

3. OPIS ULAZNIH VRIJEDNOSTI
. Identifikovane potrebe za obukom (ankete, zahtjevi rukovodilaca, rezultati ocjenjivanja)-obrazac . Ponude eksternih trenera/institucija . Budžetska sredstva (namjenska stavka) . Registar prethodno realizovanih obuka

Mape procesa

Aktivnost: Prikupljanje i analiza potreba za obukom od rukovodilaca

Kontrola: Provjera usklađenosti sa strateškim ciljevima, potpis rukovodioca OJ na zahtjevu

Aktivnost: Izrada godišnjeg plana internih i eksternih obuka

Kontrola: Provjera usklađenosti sa budžetskim sredstvima i planom nabavki, odobrenje

Aktivnost: Koordinacija sa relevantnim institucijama, provođenje postupka nabavke

Kontrola: Potpisivanje sporazuma/ugovora

Aktivnost: Vođenje registra obuka (tema, datum, polaznici, evaluacija)

Kontrola: Ograničenje pristupa ličnim podacima polaznika; redovna provjera rokova čuvanja.

Aktivnost: Evaluacija svake obuke (ispitivanje zadovoljstva, primjena znanja)

Kontrola: Kontrola da li je evaluacija sprovedena; potpisivanje izvještaja o evaluaciji; usklađivanje rezultata sa planom.

Aktivnost: Izrada godišnjeg izvještaja o obukama za rukovodioca

Kontrola: Autorizacija izvještaja od strane rukovodioca.

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI
• Godišnji plan obuka • Realizovane planirane obuke (evidencija) • Ažuriran registar obuka • Godišnji izvještaj o obukama sa preporukama

6. RESURSI/SREDSTVA
• Ljudski resursi (Službenik za ULJR, Rukovodioc,) • Budžetska sredstva (namjenska) • Prostorije za obuke (interna) • Eksterni treneri / institucije

Mape procesa

1. NAZIV PODPROCESA
Upravljanje učinkom (ocjenjivanje zaposlenih)

2. CILJ PROCESA
Kontinuirano unapređivati rezultate rada pojedinaca i cijele organizacije kroz sistem redovnog postavljanja ciljeva, praćenja i ocjenjivanja, te povezivanja ocjena sa napredovanjem i razvojem.

3. OPIS ULAZNIH VRIJEDNOSTI
• Opisi poslova (iz sistematizacije) • Godišnji ciljevi organizacione jedinice i pojedinca • Izvještaji o radu • Standardi učinka (kvaliteta, kvantitet, rokovi)

Mape procesa

Aktivnost: Postavljanje godišnjih ciljeva za svakog zaposlenog
Kontrola: Saglasnost rukovodioca OJ i zaposlenog (potpis)
Aktivnost: Praćenje rada tokom godine i evidentiranje u dosije
Kontrola: Potpis rukovodioca i zaposlenog
Aktivnost: Sprovođenje godišnjeg ocjenjivanja i izrada rješenja
Kontrola: Provjera potpunosti obrazaca; potpisivanje od strane obje strane i rukovodioca
Aktivnost: Rješavanje prigovora na ocjenu (ako postoje)
Kontrola: Formiranje nezavisne komisije
Aktivnost: Izrada izvještaja
Kontrola: Autorizacija izvještaja
Aktivnost: Povezivanje ocjena sa napredovanjem, obukama i nagrađivanjem

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI
• Ispunjeni obrasci za ocjenjivanje svakog zaposlenog • Rješenje o ocjeni • Godišnji izvještaj o upravljanju učinkom • Preporuke za obuke i napredovanje na osnovu ocjena

6. RESURSI/SREDSTVA
• Ljudski resursi (Službenik za ULJR, Rukovodioc,) • IT softver (opciono)

Mape procesa

1. NAZIV PODPROCESA
Evidencija – vođenje personalnog dosijea

2. CILJ PROCESA
Osigurati zakonito, transparentno, tačno i ažurno vođenje personalnih dosijea zaposlenih, uz poštivanje **načela minimizacije podataka, povjerljivosti i sigurnosti,** te omogućiti ostvarivanje prava i obaveza iz radnog odnosa u skladu sa regulativom.

3. OPIS ULAZNIH VRIJEDNOSTI
• Dokumentacija od strane zaposlenog/kandidata (ugovor o radu, aneksi, potvrde o stručnoj spremi, ljekarska uvjerenja, izjave, zahtjevi za ostvarivanje prava i sl.). • Evidencije i baze podataka

Aktivnost: Prijem i evidentiranje nove dokumentacije

Kontrola: Zadužena lica evidentiraju dokumentaciju

Aktivnost: Provjera zakonitosti i kompletnosti dokumentacije

Kontrola: Provjera da li postoji zakonski osnov za njeno čuvanje

Aktivnost: Sistematizacija i odlaganje dokumenata u dosije

Kontrola: Provjera fizičke zaštićenosti

Aktivnost: Uspostavljanje i ažuriranje ROPA evidencije

Kontrola: Evidentira kroz logove (elektronski) ili zapisnike (fizički)

Aktivnost: Postupanje po zahtjevima zaposlenog i trećih strana za pristup podacima

Kontrola: Provjera identiteta i prava

Aktivnost: Čuvanje dosijea i kontrola rokova (retencija)

Kontrola: Zapisnik o uništenju

Aktivnost: Prestanak radnog odnosa

Kontrola: Izdvajanje dosijea iz aktivne mape i prebacivanje u arhivu.

Mape procesa

5. OPIS IZLAZNIH VRIJEDNOSTI
• Funkcionalan i siguran personalni dosije za svakog zaposlenog, koji se sastoji od zakonito prikupljene, ažurne i relevantne dokumentacije. • Evidencije i izvještaji (ROPA, registri pristupa, evidencije zahtjeva).

6. RESURSI/SREDSTVA
Ljudski resursi HR služba, DPO (Službenik za zaštitu ličnih podataka), IT osoblje, rukovodstvo). **Materijalna sredstva** (zaključani ormari za fizičke dosijee, prostorija za povjerljive dokumente). **Tehnička sredstva** (softveri, aplikacija, sigurnosne kopije, antivirus, MFA).

Mape procesa

Podproces	Odgovorna osoba
Planiranje ljudskih resursa	**Rukovodilac organizacije** **Rukovodilac Sektora za pravne i opšte poslove**
Zapošljavanje (Regrutacija)	**Rukovodilac organizacije** **Komisija za zapošljavanje**
Obuka i razvoj	**Rukovodilac organizacije** **Rukovodilac Sektora za pravne i opšte poslove**
Upravljanje učinkom (Ocjenjivanje)	**Rukovodilac organizacije** **Rukovodioci organizacionih jedinica**
Vođenje personalnog dosijea	**Rukovodilac Sektora za pravne i opšte poslove** **Službenik za ULJR** **Ovlašteni arhivar**

Mape procesa –vježba

PROCES OBRAČUNA I ISPLATE PLAĆE - AKTIVNOSTI

- Prikupljanje podataka
- Unos podataka u program
- Obračun plata i naknada
- Ispis izvještaja iz plata i naloga za isplatu plata i naknada
- Podnošenje naloga za isplatu plata i naknada banci – elektronsko plaćanje
- Podjela isplatnih lista
- Dostavljanje mjesečnih i godišnjih izvještaja
- Arhiviranje dokumentacije

Videonadzor

Obrada ličnih podataka putem video nadzora odnosi se na prikupljanje i daljnju obradu ličnih podataka.

Videonadzorom su obuhvaćene samo prostorije ili dijelovi prostorija čiji je nadzor nužan radi postizanja bezbjednosti i zaštite imovine ljudi.

Prostori za odmor, toaleti i garderobe ne smiju biti pod video nadzorom.

Dijelovi objekta koji su pod videonadzorom moraju biti označeni na način da je oznaka vidljiva najkasnije prilikom ulaska u vidokrug snimanja.

Oznaka sadrži naznaku da je prostor pod videonadzorom, svrhu snimanja, podatke o Ustanovi (kontroloru) i kontakt podatke putem kojih nosilac podataka može ostvariti svoja prava.

Sistem video nadzora je zaštićen od pristupa neovlaštenih lica, a pravo pristupa ima samo ovlašteno lice.

Svaki snimak putem video nadzora i njihova obrada posebno se evidentira putem automatizovanog sistema zapisa sa naznačenim vremenom, mjestom pristupa i naznakom lica koje je izvršilo pristup snimcima.

Snimci dobijeni putem video nadzora čuvaju se ograničeno (najčešće do 30 dana, u skladu sa odlukom o video nadzoru), nakon čega se brišu.

Duže čuvanje je dozvoljeno samo ako je snimak izdvojen radi incidenta, disciplinskog ili sudskog postupka.

Zaključak

1.Zaštita ličnih podataka nije dodatni teret – ona je već ugrađena u vaše postojeće procese (HR, plate, IT, računovodstvo). Samo je treba prepoznati.

2.Bez mape procesa, nema ni kontrole – ako ne znate gdje su lični podaci, ne možete ih ni zaštititi.

3.Kontrolne aktivnosti su iste – autorizacija, razdvajanje dužnosti, limitiranje pristupa, logovanje – to su alati koje već koristite. Samo ih treba svjesno primijeniti na lične podatke.

4.Edukacija nije opcija, već obaveza – najveći rizik nije tehnologija, već čovjek koji ne zna šta smije, a šta ne smije.

Identifikacija ključnih rizika uz praktične primjere

22.05.2026. godine

Kontrolne aktivnosti

Mapa „MINIMUMA“ akata za javnu upravu

Neophodno je usvojiti:

- Pravilnik/politika zaštite podataka,
- Politika sigurnosti i kontrole pristupa,
- Retention politika + tabela rokova,
- Politika videonadzora (odluka + obavještenje + procedura).

Jako važno je na vrijeme uspostaviti evidencije: ROPA, evidencija zahtjeva ispitanika, registar povreda podataka, evidencija uvida/izdvajanja VN snimaka.

Neophodno je urediti odnose sa dobavljačima: DPA/ugovor o obradi + sigurnosni aneksi (logovi, pristupi, podobrađivači).

Neophodno je standardizovati obrasce: zahtjev za pristup/brisanje, prigovor, zahtjev za izdavanje podataka trećim organima, zapisnik o prijemu incidenta.

Neophodno je planirati obuke i revizije: periodična obuka + godišnja provjera primjene (audit/inspekcija internog kontrolnog organa)

Prilog 1 – Utvrđivanje rizika

NAZIV ORGANIZACIJE:	
NAZIV ORGANIZACIONE JEDINICE:	

R/br.	PROCES	CILJ	RIZIK	KATEGORIJA RIZIKA	UZROK RIZIKA	UTJECAJ / POSLJEDICA

Mjesto i datum: _____ Rukovodilac organizacione jedinice: _____

Prilog 2 – Procjena rizika

NAZIV ORGANIZACIJE:	
NAZIV ORGANIZACIONE JEDINICE:	

		OCJENA INHERENTNOG RIZIKA (Rizik ocijenjen u odsustvu bilo kakvih kontrola)						OCJENA REZIDUALNOG RIZIKA (uzimajući u obzir provedene interne kontrole / mjere za ublažavanje)			
R/br.	RIZIK	VJEROVATNOĆA (1-5)	UTJECAJ (1-5)	UKUPNO	OCJENA RIZIKA	POSTOJEĆE MJERE ZA UBLAŽAVANJE / KONTROLE	ADEKVATNOST POSTOJEĆIH MJERA ZA UBLAŽAVANJE / KONTROLE	VJEROVATNOĆA (1-5)	UTJECAJ (1-5)	UKUPNO	OCJENA RIZIKA

Mjesto i datum: _____ Rukovodilac organizacione jedinice: _____

Prilog 3 – Mjere za ublažavanje rezidualnog rizika

NAZIV ORGANIZACIJE:	
NAZIV ORGANIZACIONE JEDINICE:	

R/br.	RIZIK	VRSTA ODGOVORA NA RIZIK	DODATNE MJERE ZA UBLAŽAVANJE	REZULTAT MJERE	POTREBNI RESURSI	VLASNIK ZADATKA	ROK	VEZA S DRUGIM ORGANIZACIONIM JEDINICAMA / ORGANIZACIJAMA	PRIORITET

Mjesto i datum: _____ Rukovodilac organizacione jedinice: _____

Rizici

PROCES	CILJ	RIZIK	KATEGORIJA RIZIKA	UZROK RIZIKA	UTJECAJ / POSLJEDICA
Zapošljavanje (prijem u radni odnos)	**Popunjavanje upražnjenih radnih mjesta, osobama sa potrebnim kvalifikacijama i kompetencijama, kroz zakonit, transparentan i fer postupak, uz punu zaštitu ličnih podataka kandidata.**	1.1. Uslijed nepoznavanja zakonskih procedura, dolazi do neusklađenosti konkursa sa regulativom, što za posljedicu ima žalbe kandidata, poništenje konkursa i troškove ponavljanja postupka.	Pravni rizik	- Nedostatak interne procedure - Izmjene propisa bez obuke - Nema pravne provjere prije objave	- Žalbe, sudski sporovi - Odgađanje popunjavanja radnog mjesta - Šteta po ugled
		1.2. Nekoordinacija između kadrovske i finansijske službe prilikom planiranja dovodi do raspisivanja konkursa bez osiguranih budžetskih sredstava što za posljedicu ima otežano poslovanje organizacije.	Operativni rizik	- Nekoordinacija - Kasna dostava informacija	- Dodatni troškovi, - Neizvršavanje zakonskih obaveza - Tužbe
		1.3. Zbog nepostojanja internih pravila o zaštiti podataka i zajedničkog pristupa prijavama, dolazi do neovlaštenog otkrivanja ličnih podataka kandidata (CV, JMBG), što za posljedicu ima kaznu Agencije za zaštitu ličnih podataka i odštetne zahtjeve.	Pravni rizik	- Zajednički e-mail, nezaštićeni folderi - Nema logova pristupa	- Kazna (do 2% prihoda) - Tužbe kandidata - Gubitak reputacije

Rizici

PRIJEDLOG PODRUČJA KOJA SE MOGU UZIMATI U OBZIR KADA SE UTVRĐUJU RIZICI

1. **Eksterno okruženje**

- ✓ Rizici makro okruženja (geopolitički, ekonomski, prirodne katastrofe, i sl.)
- ✓ Političke odluke i prioriteti izvan organizacije (Parlament, Vijeće, i sl.)
- ✓ Spoljni partneri (građani, druge institucije javnog sektora, spoljni pružaoci usluga, mediji, i sl.)

2. **Planiranje, procesi, sistemi**

- ✓ Strategije, planiranje i interne politike
- ✓ Operativni procesi (dizajn i opis procesa)
- ✓ Finansijski sistemi i raspodjela sredstava
- ✓ IT i ostali sistemi podrške

Rizici

PRIJEDLOG PODRUČJA KOJA SE MOGU UZIMATI U OBZIR KADA SE UTVRĐUJU RIZICI

3. **Zaposleni i organizacija**

- ✓ Zaposleni, njihove vještine i stručnost
- ✓ Etika i ponašanje organizacije („ton s vrha", politike protiv prevara, sukob interesa)
- ✓ Interna organizacija (upravljanje, uloge i odgovornosti, delegiranje)
- ✓ Bezbjednost zaposlenih, objekata i opreme

4. **Zakonitost i pravilnost**

- ✓ Jasnoća, usklađenost i specifičnost postojećih zakona, propisa i pravila
- ✓ Ostali mogući ishodi koji se odnose na zakonitost i pravilnost

5. **Komunikacija i informacije**

- ✓ Metode i kanali komuniciranja
- ✓ Kvalitet i blagovremenost informacija

Rizici

Rizik	Zašto baš ovaj?
1.1. Neusklađenost sa regulativom	**Jer je proces zapošljavanja najregulisaniji proces u organizaciji.** Zakon o radu, zakon o državnoj službi, pravilnici – svaka greška je žalba i poništenje konkursa.
1.2. Nekoordinacija sa finansijskom službom	**Jer bez novca nema ni zaposlenja.** Ako kadrovska raspise konkurs a finansijska nema budžet – odabranog kandidata ne možete primiti.
1.3. Otkrivanje ličnih podataka	**Jer su prijave kandidata (CV, JMBG) osjetljivi podaci po zakonu.** Zajednički email i nezaštićeni folderi su direktan prekršaj koji nosi ogromne kazne.

Rizici

		OCJENA INHERENTNOG RIZIKA						OCJENA REZIDUALNOG RIZIKA			
R/br.	RIZIK	VJEROVATNOĆA	UTICAJ	UKUPNO	OCJENA RIZIKA	POSTOJEĆE MJERE ZA UBLAŽAVANJE / KONTROLE	ADEKVATNOST POSTOJEĆIH MJERA ZA UBLAŽAVANJE / KONTROLE	VJEROVATNOĆA	UTICAJ	UKUPNO	OCJENA RIZIKA
1.1.	Uslijed nepoznavanja zakonskih procedura, dolazi do neusklađenosti konkursa sa regulativom, što za posljedicu ima žalbe kandidata, poništenje konkursa i troškove ponavljanja postupka.	4	4	16	Visok	Pravilnik o radu	Djelimično zadovoljavajuće	2	4	9	Srednji
1.2.	Nekoordinacija između kadrovske i finansijske službe prilikom planiranja dovodi do raspisivanja konkursa bez osiguranih budžetskih sredstava što za posljedicu ima otežano poslovanje organizacije.	3	5	15	Visok	Godišnji budžet/finansijski plan Plan zapošljavanja Finansijska služba daje mišljenje	Zadovoljavajuće	2	3	6	Nizak
1.3.	Zbog nepostojanja internih pravila o zaštiti podataka i zajedničkog pristupa prijavama, dolazi do neovlaštenog otkrivanja ličnih podataka kandidata (CV, JMBG), što za posljedicu ima kaznu Agencije za zaštitu ličnih podataka i odštetne zahtjeve.	4	5	20	Kritičan	Opšti pravilnik o radu Konkursna komisija	Djelimično zadovoljavajuće	3	5	15	Visok

Rizici

Jednostavno rečeno:

Smanjenje vjerovatnoće = zaključaj vrata da lopov ne uđe.
Smanjenje uticaja = pripremi šta ćeš raditi ako lopov ipak provali.

Mjere za smanjenje VJEROVATNOĆE (spriječiti grešku)

- Godišnja obuka kadrovske službe o izmjenama radnog zakonodavstva
- Obavezna pravna provjera teksta oglasa prije objave (kontrolna lista)
- Sertifikacija službenika za provođenje konkursnih postupaka
- Evidencija žalbi i poništenih konkursa radi učenja na greškama
- **Anonimizacija prije bodovanja**

Mjere za smanjenje UTICAJA (kada se greška desi)

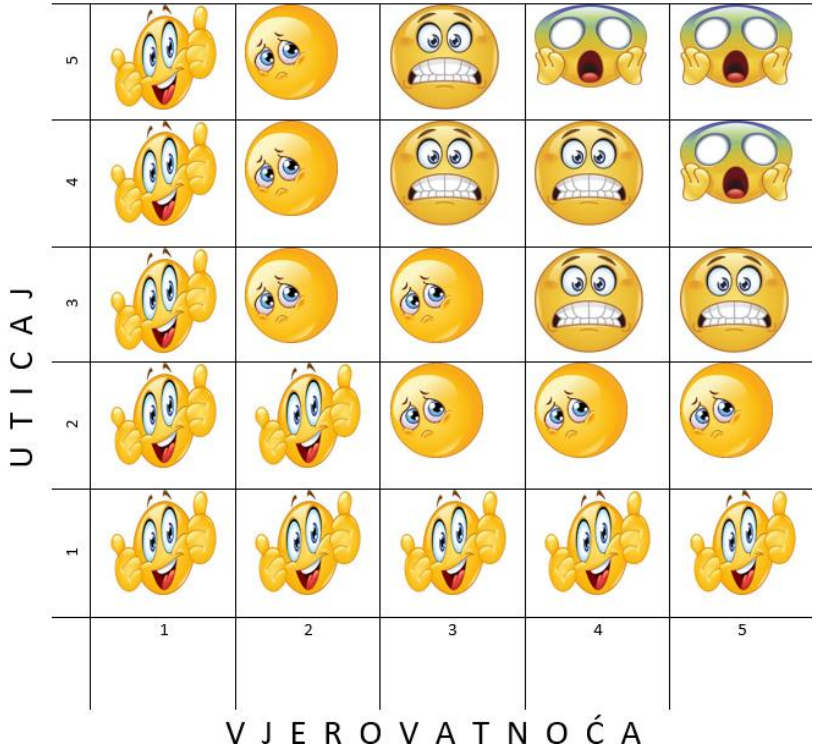
- Šablon za brzu izmjenu oglasa – pripremljen unaprijed
- Budžetska rezerva za pokrivanje troškova ponavljanja konkursa
- Istorijat konkursa
- Privremeno rješenje (npr. ugovor na određeno) dok se konkurs ne ponovi
- **Protokol za prijavu incidenta**

Rizici

RIZIK	VRSTA ODGOVORA NA RIZIK	DODATNE MJERE ZA UBLAŽAVANJE	REZULTAT MJERE	POTREBNI RESURSI	VLASNIK ZADATKA	ROK	VEZA S DRUGIM ORGANIZACIONIM JEDINICAMA / ORGANIZACIJAMA	PRIORITET
Uslijed nepoznavanja zakonskih procedura , dolazi do neusklađenosti konkursa sa regulativom, što za posljedicu ima žalbe kandidata, poništenje konkursa i troškove ponavljanja postupka.	Smanjenje	Donijeti interni pravilnik o provođenju konkursa sa rokovima i obrascim Lista kontrole (checklist) prije objave konkursa, obuku o radnom pravu	Usvojen pravilnik sa obrscem, potvrde o obuci	Obuka 500 KM	Kadrovska služba	2 mjeseca	-	Visok
Zbog nepostojanja internih pravila o zaštiti podataka i zajedničkog pristupa prijavama, dolazi do neovlaštenog otkrivanja ličnih podataka kandidata (CV, JMBG), što za posljedicu ima kaznu Agencije za zaštitu ličnih podataka i odštetne zahtjeve.	Smanjenje	Uspostaviti poseban e-mail za konkurse (pristup samo članovima komisije); potpisati izjave o povjerljivosti; logovati pristup	Funkcionala n e-mail, potpisane izjave, logovi	-	Kadrovska služba	1 mjesec	IT sektor	Visoki

APETIT ZA RIZIK

Količina rizika koju je neka organizacija spremna prihvatiti, tolerisati ili biti mu izložena u bilo kojem trenutku.
Rizik je neizbježan i svaka organizacija treba poduzeti radnje vezane uz upravljanje rizicima na način da može opravdati nivo do koje ga toleriše.



Tri razloga zašto baš ova tri rizika

Rizici

PROCES	CILJ	RIZIK	KATEGORIJA RIZIKA	UZROK RIZIKA	UTJECAJ / POSLJEDICA
Upravljanje životnim ciklusom IT sistema	Osigurati planiranje, razvoj, implementaciju, održavanje i povlačenje IT sistema na kontrolisan, siguran i usklađen način, uz zaštitu podataka i efikasno upravljanje resursima.	Zastarjeli hardver uzrokuje prekide rada, što dovodi do prekida poslovanja i dodatnih troškova popravki	Operativni	- Nema plana zamjene - Nedostatak budžeta	- Prekid poslovanja (sati/dani) - Dodatni troškovi popravki
		Kibernetički napad (ransomware, phishing) uzrokuje gubitak i curenje podataka, plaćanje otkupnine te kazne i tužbe	Operativni	- Slaba antivirus zaštita - Nema MFA - Zaposlenici neobučeni	- Gubitak/curenje podataka - Otkupnina - Kazne, tužbe
		Gubitak podataka usljed kvara diska (bez backupa) uzrokuje nepovratan gubitak svih podataka i prekid rada	Operativni	- Backup nepostojeći ili na istoj lokaciji - Nema testiranja restauracije	- Nepovratni gubitak svih podataka - Prekid rada
		Neovlašten pristup podacima od strane IT servisera (vanjska firma) uzrokuje curenje povjerljivih podataka i kaznu Agencije	Pravni	- Nema potpisanog DPA ugovora - Serviser ima admin pristup bez nadzora	- Curenje povjerljivih podataka - Kazna Agencije

Tri razloga zašto baš ova tri rizika

Pravna i ekonomska izdanja za uspješno i zakonito poslovanje

Rizici

BUDITE NA PRAVNOJ STRANI

www.paragraf.ba - www.paragraf.rs

R/br.	RIZIK	VJEROVATNOĆA	UTJECAJ	UKUPNO	OCJENA RIZIKA	POSTOJEĆE MJERE ZA UBLAŽAVANJE / KONTROLE	ADEKVATNOST POSTOJEĆIH MJERA ZA UBLAŽAVANJE / KONTROLE	VJEROVATNOĆA	UTJECAJ	UKUPNO	OCJENA RIZIKA
1.	Zastarjeli hardver uzrokuje prekide rada, što dovodi do prekida poslovanja i dodatnih troškova popravki	4	4	16	Visok	Redovno održavanje	Djelimično zadovoljavajuća	3	4	12	Visok
2.	Kibernetički napad (ransomware, phishing) uzrokuje gubitak i curenje podataka, plaćanje otkupnine te kazne i tužbe	4	5	20	Kritičan	Antivirus, lozinke, cloud server	Nezadovoljavajuće	4	4	16	Visok
3.	Gubitak podataka usljed kvara diska uzrokuje nepovratan gubitak svih podataka i prekid rada	5	5	25	Kritičan	Automatski backup na odvojenoj lokaciji (cloud server), test restauracije kvartalno	Zadovoljavajuća	2	2	4	Nizak

Rizici

R/br.	RIZIK	VJEROVATNOĆA	UTJECAJ	UKUPNO	OCJENA RIZIKA	POSTOJEĆE MJERE ZA UBLAŽAVANJE / KONTROLE	ADEKVATNOST POSTOJEĆIH MJERA ZA UBLAŽAVANJE / KONTROLE	VJEROVATNOĆA	UTJECAJ	UKUPNO	OCJENA RIZIKA
4.	Neovlašten pristup podacima od strane IT servisera (vanjska firma) uzrokuje curenje povjerljivih podataka i kaznu Agencije	4	5	20	Kritičan	Ugovor sa serviserom (bez DPA)	Djelimično zadovoljavajuća	3	5	15	Visok

Tri razloga zašto baš ova tri rizika

Rizici

RIZIK	VRSTA ODGOVORA NA RIZIK	DODATNE MJERE ZA UBLAŽAVANJE	REZULTAT MJERE	POTREBNI RESURSI	VLASNIK ZADATKA	ROK	VEZA S DRUGIM ORGANIZACIONIM JEDINICAMA / ORGANIZACIJAMA	PRIORITET
Zastarjeli hardver uzrokuje prekide rada, što dovodi do prekida poslovanja i dodatnih troškova popravki	Smanjenje	Donijeti plan zamjene IT opreme za 3 godine, osigurati budžetsku stavku,	Usvojen plan zamjene, ažuriran hardver	Budžetska sredstva za nabavku opreme (50.000 KM), angažman IT osoblja	IT rukovodilac	3 mjeseca	Finansije	Visok
Kibernetički napad (ransomware, phishing) uzrokuje gubitak i curenje podataka, plaćanje otkupnine te kazne i tužbe	Smanjenje i prenošenje	Uvesti MFA za sve korisnike, zaključiti policu osiguranja od kibernetičkih rizika, obučiti sve zaposlene o phishing-u	Implementirana MFA, potpisana polica osiguranja, provedena obuka	Sredstva za MFA licence (do 2.000 KM), premija osiguranja, edukativni materijali	IT rukovodilac	2 mjeseca	Finansije	Visok
Neovlašten pristup podacima od strane IT servisera (vanjska firma) uzrokuje curenje povjerljivih podataka i kaznu Agencije	Smanjenje	Zaključiti DPA ugovor sa IT serviserom, ograničiti mu pristup samo uz nadzor (logove), uvesti evidenciju pristupa	Potpisan DPA, uspostavljeni logovi i evidencija	-	IT rukovodilac	1 mjesec	Pravna služba	Visok

PROCJENA RIZIKA

Procjena i kvantitativna analiza rizika

Za rizike koji su na osnovu kvalifikacione analize (procjene vjerovatnoće i uticaja) rangirani kao visoki prioritet, sprovodi se procjena metrika uticaja rizika, najčešće vezana za finansijske štete, dodatne troškove i gubitke prihoda. Ova analiza se obavlja kvantitativno.

Kvantitativna analiza
Kvantitativna analiza odgovara na pitanje „šta ako“ se rizik dogodi, procjenjujući šanse za postizanje ciljeva uz minimalne negativne efekte. Uključuje podatke o troškovima, prihodima, historijskim događajima i relevantnoj statistici. Analize se sprovode kroz razgovore među zaposlenicima, procjene monetarne vrijednosti, analize odluka i izradu scenarija.

PROCJENA RIZIKA

Scenario: Razmotrite sljedeći primjer vezan za kapitalnu investiciju koja premašuje početni budžet. U okviru vježbe, analizirajte rizike i izračunajte ukupne troškove povezane s njima.

Kapitalna investicija vrijednosti 2.000.000,00 KM

- Prekoračenje početnog budžeta za 10%.
- Kašnjenje na otkupu zemljišta vremenski period: 2 godine. Vjerovatnoća: 80% (na osnovu prošlog iskustva i pregleda).
- Penali za neiskorištena kreditna sredstva: 2% od iznosa od 2.000.000 KM.
- Kašnjenje u javnoj nabavci vremenski period: 0,5 godina. Vjerovatnoća: 70% (prosječan broj odgođenih javnih nabavki i prosječno kašnjenje za projekte izgradnje mostova). Finansijski uticaj: 20.000 KM.
- Kašnjenje zbog klizišta i dodatnih radova vremenski period: 0,4 godine. Dodatni troškovi: 5%. Vjerovatnoća: 50% (na osnovu prethodnog iskustva). Osnovni trošak za dodatne radove: 100.000 KM.

PROCJENA RIZIKA

Odgovor na zadatak o kvantifikaciji rizika kapitalne investicije:

- Premošenje početnog budžeta 10% od početnog budžeta. **Trošak: 2.000.000×0.10=200.000**
- Kašnjenje na otkupu zemljišta, penali za neiskorištena kreditna sredstva: 2.000.000×0.02=40.000 KM
  Ukupan trošak (vjerovatnoća 80%): **40.000×0.80=32.000 KM**
- Kašnjenje u javnoj nabavci Finansijski uticaj: 20.000 KM
- Ukupan trošak (vjerovatnoća 70%): **20.000×0.70=14.000 KM**
- Kašnjenje zbog klizišta i dodatnih radova. Dodatni troškovi: 100.000×0.05=5.000 KM

Ukupan trošak (vjerovatnoća 50%): 5.000×0.50=2.500 KM.

Procjena ukupnog finansijskog uticaja svih rizika
Ukupni troškovi povezani sa rizicima:
Premošenje budžeta: 200.000 KM
Kašnjenje na otkupu: 32.000 KM
Kašnjenje u javnoj nabavci: 14.000 KM
Kašnjenje zbog klizišta: 2.500 KM

Ukupno: **248.500 KM**

UZROK

Analiza glavnih **uzroka** rizika pomoći će razjasniti okruženje rizika i odrediti pristupe za ublažavanje rizika, a pomoći će i reviziji internih kontrola i drugih mjera ublažavanja rizika u smislu njihove adekvatnosti. Pitanje „ZAŠTO“

Metoda 5 X Zašto

Problem: Nedostaju sredstva za obnovu školske infrastrukture.

1. Zašto nedostaju sredstva za obnovu školske infrastrukture

Zato što postoje znatni nedostaci i oštećenja u postojećim školskim zgradama.

2. Zašto postoje znatni nedostaci i oštećenja u školskim zgradama?

Zato što su školske zgrade stare i nisu redovno održavane.

3. Zašto školske zgrade nisu redovno održavane?

Zato što postoji ograničenje budžeta za održavanje škole.

4. Zašto postoji ograničenje budžeta za održavanje školskih zgrada?

Zato što političke odluke nisu uzimale u obzir potrebe školske infrastrukture.

5. Zašto političke odluke nisu u potpunosti uzimale u obzir potrebe školske infrastrukture?

Zato što nedostaju dugoročne strategije za održavanje škola.

Rizici –vježba

PROCES OBRAČUNA I ISPLATE PLAĆE

Zaključak

1. Rizik nije vaš neprijatelj – nekontrolisani rizik jeste. Apetit za rizik je nešto što svaka organizacija mora svjesno da definiše.

2. Ne možete upravljati onim što niste zapisali – zato je registar rizika obavezan, a ne samo „još jedna tabla “.

3. Razlikujte vjerovatnoću i uticaj – neke rizike ne možete spriječiti, ali možete ublažiti posljedicu. To je ono što profesionalca razlikuje od amatera.

4. **Kvantitativna analiza nije samo za finansijski sektor** – kada izračunate koliko vas košta jedan poništen konkurs, jedna kazna Agencije ili jedan ransomware napad, shvatite da je ulaganje u upravljanje rizicima– investicija, a ne trošak.

Matrica-primjer

Oznaka	Značenje
Čitanje	Može pogledati podatke
Unošenje	Može dodati ili promijeniti podatke
Brisanje	Može trajno obrisati podatke
Vlasništvo	Može drugima dati ili oduzeti dozvolu nad tim podacima
Nadzor	Može kontrolisati šta drugi rade, ali ne mora imati sva prava
Tehnički pristup	Može pristupiti samo radi održavanja sistema, ne smije čitati sadržaj bez odobrenja

Matrica-primjer

o (domen) → Šta (objekat) ↓	Kadrovska služba	Računovodstvo	IT služba	Rukovodilac odjela	DPO	Eksterni servis (npr. obračun plata)
Personalni dosije (JMBG, adresa, djeca)	Čitanje, Unošenje, Brisanje, Vlasništvo	–	–	Čitanje (samo za svoje radnike)	Čitanje, Nadzor	–
Platne liste	Čitanje, Unošenje	Čitanje, Unošenje, Brisanje, Vlasništvo	–	Čitanje (zbirno)	Čitanje, Nadzor	Unošenje (po ugovoru)
Evidencija radnog vremena	Čitanje, Unošenje	–	Tehnički pristup	Čitanje (svoj tim)	Čitanje, Nadzor	–
Snimci videonadzora	–	–	Tehnički pristup, Nadzor	Čitanje (uz obrazloženje)	Čitanje, Nadzor	–
Logovi pristupa (ko je gledao podatke)	–	–	Čitanje, Unošenje, Nadzor	–	Čitanje, Nadzor	–
Saglasnosti radnika	Čitanje, Unošenje, Vlasništvo	–	–	Čitanje (svoj tim)	Čitanje, Nadzor	