Naziv: DJEČJI VRTIĆ LOPTICA,
Adresa sjedišta: Tina Ujevića 12, 40000 Čakovec
OIB: OIB: 75764016426

Kontakt telefon: +385 99 3713 980
Elektronička pošta: djecji.vrtic.loptica@gmail.com

PROCJENA UČINKA NA ZAŠTITU PODATAKA
ANALIZA RIZIKA
19.01.2021.

NAZIV DOKUMENTA:	**ANALIZA RIZIKA**
REFERENCA:	GDPR-RIZIK-2021
DOKUMENT IZRADIO:	**Azziris,** obrt za savjetovanje Varaždin
VODITELJ OBRADE:	**DJEČJI VRTIĆ LOPTICA,** Čakovec

Povijest verzija

Verzija	Datum	Izradio	Opis / sažetak izmjena
1	20.01.2020	Helena Hunjak Sirovec	Početna verzija izrađena prilikom implementiranja GDPR regulative
2	19.01.2021.	Helena Milfelner	Procjena učinka i analiza rizika 2021

SADRŽAJ

1. UVOD

1.1. Namjena Analize

Ova Analiza rizika sigurnosti osobnih podataka utvrđuje djelotvoran, odgovoran i transparentan okvir za osiguravanje usklađenosti s Općom uredbom o zaštiti osobnih podataka.koja se primjenjuju u svim obradama osobnih podataka koje provodi Dječji vrtić Loptica, Tina Ujevića 12, 40000 Čakovec *OIB:* 75764016426 (u daljnjem tekstu: Voditelj obrade). Ista se primjenjuje na na sve zaposlenike, uključujući honorarne djelatnike i privremene radnike jednako kao i na sve vanjske suradnike koji sudjeluju u ime Voditelja obrade.
Voditelj obrade djeluje na sljedećim lokacijama te se ova analiza odnosi na sve lokacije djelovanja voditelja obrade:

1. Dječji vrtić Loptica - Čakovec
2. Područni odjel Medo – Orehovica

Prilikom procjene rizika za sigurnost podataka u obzir se uzimaju rizici koje predstavlja obrada osobnih podataka poput slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog odavanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, a što osobito može dovesti do fizičke, materijalne ili nematerijalne štete.
Cilj analize rizika je provjera sukladnosti sustava upravljanja zaštitom osobnih podataka s Općom uredbom o zaštiti podataka (GDPR) i Zakonom o provedbi Opće uredbe o zaštiti podataka, u dijelu smanjivanja rizika povezanih s obradama osobnih podataka, te stalnim unapređenjem sustava sigurnosti i zaštite osobnih podataka.
Redovita provjera usklađenosti sustava predstavlja sustavni, neovisni i dokumentirani proces za pribavljanje dokaza i njihovo objektivno ocjenjivanje da bi se odredilo do koje mjere su ispunjeni kriteriji provjere.
Voditelj obrade kvalitativnom i kvantitativnom analizom rizika procjenjuje da o kakvom se riziku radi kod obrade osobnih, te određuje fizičke, tehničke i organizacijske mjere koje su potrebe kako bi se rizik kod obrade osobnih podataka umanjio.

1.2. Referentni dokumenti

- Opća uredba o zaštiti podataka (GDPR) UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. godine,
- Direktiva o privatnosti u elektroničkim komunikacijama (Direktiva 2002/58/EC),
- Zakon o provedbi Opće uredbe o zaštiti podataka (805) NN 42/2018 od 27. travnja 2018. godine
- Pravilnik o zaštiti osobnih podataka (primjena od 31.12.2019.)
- Procedura za obradu zahtjeva u vezi osobnih podataka (primjena od 31.12.2019.)
- Procedura za postupanje kod povrede osobnih podataka (primjena od 31.12.2019.)
- Evidencija aktivnosti obrade (primjena od 31.12.2019.)
- Politika privatnosti
- Politika sigurnosti osobnih podataka
- Informacija o privatnosti za zaposlenike (kadrovska usklađenost)
- Analiza rizika
- Program provjere usklađenosti

2. Definiranje rizika

U običnom razgovoru rizik se često koristi kao sinonim za mogućnost gubitka ili opasnost. U procjeni rizika koncept rizika kombinira vjerojatnost događaja s utjecajem koji taj događaj može imati na imovinu u različitim okolnostima događanja.
U ovoj analizi imovina koju Voditelj želi zaštiti su osobni podaci koje obrađuje.

2.1. Praćenje rizika i izvješćivanje o rizicima

Upravljanje rizicima kontinuirani je proces koji treba uključiti praćenje utvrđenih rizika kako bi se pravodobno uočile sve promjene vezane uz rizike (npr. pojava novih rizika i mogućih prilika koje se javljaju uz rizike).
Budući da se poslovno, ekonomsko i zakonodavno okruženje neprestano mijenja, mijenja se i okruženje svakog rizika pa će se mijenjati i prioriteti ciljeva i značaj pridruženih rizika.
Zbog navedenog, rizike treba redovito pregledavati i razmatrati kako bi se zadržala učinkovitost odgovora na rizik.
Također je potrebno obavljati stalne preglede kako bismo bili sigurni da su svi rizici povezani s ciljevima te da su svi ciljevi uzeti u obzir pri utvrđivanju i ažuriranju rizika.
Procijenjene rizike treba pregledavati i o tome izvješćivati radi stjecanja sigurnosti o djelotvornosti upravljanja rizicima te kako bi se utvrdile situacije u kojima su potrebne druge radnje.

3. PROCJENA UČINKA NA ZAŠTITU PODATAKA

Obveza provođenja procjene učinka na zaštitu podataka primjenjuje se na postojeće postupke obrade, koji će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca i u pogledu kojih je došlo do promjene rizika, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade.

Radna skupina za zaštitu podataka iz članka 29. Uredbe smatra da procjena učinka na zaštitu podataka nije potrebna u slijedećim slučajevima:

- ako obrada vjerojatno neće prouzročiti visok rizik za prava i slobode pojedinaca (članak 35. stavak 1.),

- ako su priroda, opseg, kontekst i svrhe obrade jako slični obradi za koju je procjena učinka na zaštitu podataka bila provedena. U takvim slučajevima, mogu se koristiti rezultati procjene učinka na zaštitu podataka za slične obrade (članak 35. stavak 1.19),

- ako je postupke obrade provjerilo nadzorno tijelo prije svibnja 2018. u posebnim uvjetima koji se nisu promijenili,

- ako postupak obrade, u skladu sa člankom 6. stavkom 1. točkom (c) ili (e), ima pravni temelj u zakonodavstvu EU-a ili države članice, ako je zakonodavstvom uređen poseban postupak obrade i ako je procjena učinka na zaštitu podataka već bila provedena kao dio uspostave tog pravnog temelja (članak 35. stavak 10.), osim ako je država članica zahtijevala provođenje procjene učinka na zaštitu podataka prije aktivnosti obrade,

- ako je obrada uvrštena na fakultativni popis postupaka obrade (koji je uspostavilo nadzorno tijelo) za koje nije potrebna procjena učinka na zaštitu podataka (članak 35. stavak 5.)

S obzirom na postavljene kriterije koje Voditelj obrade ne zadovoljava nije potrebno provoditi Procjenu učinka na zaštitu podataka. U nastavku dajemo pripremu za procjenu učinka za zaštitu podataka ukoliko će biti zadovoljen neki od gore navedenih kriterija.

PROCJENA UČINKA NA ZAŠTITU PODATAKA	OPIS
1. Sustavan opis obrade (članak 35. (7) (a)):	
a) priroda, opseg, kontekst i svrhe obrade koje se uzimaju u obzir (uvodna odredba 90);	
b) osobni podaci, ispitanici i razdoblje na koje se osobni podaci pohranjuju ili bilježe;	
c) funkcionalni opis operacije obrade;	
d) sredstva na koja se osobni podaci oslanjaju (hardver, softver, mreže, osobe, papir, papirni prijenosni kanali);	
2. Procjena nužnosti i proporcionalnosti (članak 35 (7) (b)):	
a) mjere predviđene radi usklađivanja s Uredbom (članak 35 (7) (d) i uvodna odredba 90), uzimajući u obzir:	
i. Mjere koje doprinose proporcionalnosti i nužnosti obrade temeljem:	
(-) posebne, izričite i zakonite svrhe(a) (članak 5 (1) (c));	
(-) zakonitosti obrade (članak 6);	
(-) primjerenosti, relevantnosti i ograničenosti na nužne podatke (članak 5(1) (c));	
(-) ograničenja pohrane (članak 5 (1) (e));	
ii. Mjere koje doprinose proporcionalnosti i nužnosti obrade temeljem:	
(-) informacija koje se daju ispitanicima (članci 12, 13 i 14)	
(-) prava na pristup i prenosivost (članci 15 i 20);	
(-) prava na ispravak, brisanje, prigovor, ograničenje obrade (članci 16 do 19 i 21);	
(-) ispitanika;	
(-) izvršitelja obrade (članak 28);	
(-) zaštitnih mjera u vezi međunarodnog prijenosa (Poglavlje V);	
(-) prethodnog savjetovanja (članak 36).	
3. Rizici za prava i slobode ispitanika (članak 35 (7) (c));	
a) izvor, priroda, osobitost i ozbiljnost rizika (uvodna odredba 84) ili, preciznije, za svaki rizik (nedozvoljeni pristup, neželjena izmjena i nestanak podataka) iz perspektive ispitanika:	
i. izvori rizika koji se uzimaju u obzir (uvodna odredba 90);	
ii. moguće posljedice za prava i slobode ispitanika identificirane u slučaju nedozvoljenog pristupa, neželjene izmjene i nestanka podataka;	
iii. prijetnje koje mogu dovesti do nedozvoljenog pristupa, neželjene izmjene i nestanka podataka;	
iv. vjerojatnost i ozbiljnost (uvodna odredba 90); učinak rizika	
b) mjere predviđene za tretiranje tih rizika (članak 35 (7) (d)) i uvodna odredba 90);	
4. Zainteresirane strane:	
a) traži se savjet službenika za zaštitu podataka (članak 35 (2));	
b) traži se mišljenje ispitanika ili njihovih predstavnika (članak 35 (9));	
Ako se procjena učinka na zaštitu podataka pokazuje da bi obrada dovela do visokog rizika u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, voditelj obrade će se savjetovati s nadležnim nadzornim tijelom prije obrade (članak 36)	

4. ANALIZA RIZIKA

4.1. Krađa osobnih podataka unutar/izvan organizacije

<table>
<tr><td>NAZIV RIZIKA</td><td colspan="10">Krađa osobnih podataka unutar/izvan organizacije</td></tr>
<tr><td>OPIS PRIJETNJE / RIZIKA</td><td colspan="10">Provala u ured voditelja obrade
Krađa papirnate dokumentacije / Krađa IT opreme
Krađa podataka od strane djelatnika</td></tr>
<tr><td>IZBJEGAVANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRENOŠENJE RIZIKA</td><td colspan="10">Ugovaranje police osiguranja imovine od osnovnih rizika (požar i druge opasnosti) i dopunskih rizika (krađe)</td></tr>
<tr><td>PRIHVAĆANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>SMANJENJE / UBLAŽAVANJE RIZIKA</td><td colspan="10">Definiranje fizičkih sigurnosnih barijera -zaključavanje ulaznih vrata u poslovne prostore
Odlaganje papirne dokumentacije u zaključane ormare i ladice
Smještaj IT opreme i dokumentacije u zaštićene prostorije s ograničenim pristupom (sigurne sobe)
Korištenje lozinki za ulaz u računalo
Ne davanje vlastite lozinke drugim zaposlenicima
Educiranje zaposlenika
Podizanje zadovoljstva zaposlenika
Održavanje dobre radne klime i timskog rada
Kontinuirana pohrana sigurnosnih kopija</td></tr>
<tr><td rowspan="3">IZVOR/UZROK PRIJETNJE</td><td colspan="9">PRIRODNI</td><td></td></tr>
<tr><td colspan="9">TEHNIČKI</td><td></td></tr>
<tr><td colspan="9">LJUDSKI FAKTOR – unutarnji i vanjski</td><td>X</td></tr>
<tr><td>POSTOJEĆE MJERE ZA SMANJENJE RIZIKA</td><td colspan="10"><u>PREVENTIVNA KONTROLA</u>
Nakon završetka svakog radnog dana:
- Provjeriti jesu li zaključana ulazna vrata u poslovni prostor nakon napuštanja sjedišta OPG-a
- papirnu dokumentaciju zaključati u ormare i ladice
<u>DETEKTIVNA KONTROLA</u>
Kontrola pohrane sigurnosnih kopija
Kontrola promjene lozinki</td></tr>
<tr><td rowspan="2">PROCJENA RAZINE RIZIKA</td><td colspan="3">Vjerojatnost</td><td colspan="3">Učinak</td><td colspan="3">Rizik</td></tr>
<tr><td>Malo vjerojatno</td><td>Vjerojatno</td><td>Vrlo vjerojatno</td><td>Niski utjecaj</td><td>Značajan utjecaj</td><td>Visok utjecaj</td><td>Niski</td><td>Srednji</td><td>Visok</td></tr>
<tr><td>X</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>MJERE KOJE ĆE SE PODUZETI ZA SMANJENJE RIZIKA</td><td colspan="10">Ugovaranje police osiguranja imovine od osnovnih rizika (požar i druge opasnosti) i dopunskih rizika (krađe)
implementirana kontrola pristupa
disciplinski postupak - Obavještavanje vlasnika o nastalom incidentu</td></tr>
<tr><td rowspan="2">UTJECAJ MJERA NA RIZIK</td><td colspan="3">Eliminiran rizik</td><td colspan="3">Smanjen rizik</td><td colspan="3">Prihvaćen rizik</td></tr>
<tr><td colspan="3"></td><td colspan="3">X</td><td colspan="3"></td></tr>
</table>

4.2. Povreda osobnih podataka od strane ovlaštenih osoba

<table>
<tr><td>NAZIV RIZIKA</td><td colspan="10">Povreda osobnih podataka od strane ovlaštenih osoba</td></tr>
<tr><td>OPIS PRIJETNJE / RIZIKA</td><td colspan="10">Brisanje / uništenje podataka – ljudska pogreška ili namjerno uništenje
Zaposlenik/ ovlaštena osoba koji ima pristup osobnim podacima iste prosljeđuje neovlaštenoj osobi
Nekontrolirana izmjena osobnih podataka od strane ovlaštene osobe
Odavanje osobnih podataka od strane ovlaštenih osoba</td></tr>
<tr><td>IZBJEGAVANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRENOŠENJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRIHVAĆANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>SMANJENJE / UBLAŽAVANJE RIZIKA</td><td colspan="10">Korištenje lozinki
Ne davanje vlastite lozinke drugim zaposlenicima
Oprema korisnika pravilno zaštićena
Educiranje zaposlenika i rad na integritetu djelatnika
Razvijanje svijesti, trening i edukacija o značaju vrijednosti osobnih podataka
Podizanje zadovoljstva zaposlenika
Održavanje dobre radne klime i timskog rada
Kontinuirana pohrana sigurnosnih kopija</td></tr>
<tr><td rowspan="3">IZVOR/UZROK PRIJETNJE</td><td colspan="9">PRIRODNI</td><td></td></tr>
<tr><td colspan="9">TEHNIČKI – kvar opreme</td><td>X</td></tr>
<tr><td colspan="9">LJUDSKI FAKTOR – unutarnji</td><td>X</td></tr>
<tr><td>POSTOJEĆE MJERE ZA SMANJENJE RIZIKA</td><td colspan="10"><u>PREVENTIVNA KONTROLA</u>
Upoznavanje svih zaposlenika s Politikom privatnosti
Za svakog novog djelatnika osigurati edukaciju o radu sa osobnim podacima.
Kontinuirano jednom godišnje - Organizirati podizanje radne kvalitete, team-bulding.

<u>DETEKTIVNA KONTROLA</u>
Kontrola pohrane sigurnosnih kopija
promjene lozinki</td></tr>
<tr><td rowspan="2">PROCJENA RAZINE RIZIKA</td><td colspan="3">Vjerojatnost</td><td colspan="3">Učinak</td><td colspan="3">Rizik</td></tr>
<tr><td>Malo vjerojatno</td><td>Vjerojatno</td><td>Vrlo vjerojatno</td><td>Niski utjecaj</td><td>Značajan utjecaj</td><td>Visok utjecaj</td><td>Niski</td><td>Srednji</td><td>Visok</td></tr>
<tr><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>MJERE KOJE ĆE SE PODUZETI ZA SMANJENJE RIZIKA</td><td colspan="10">Potpisana izjava o povjerljivosti
Disciplinski postupak za kršenje sigurnosti -obavještavanje vlasnika o nastalom incidentu
Implementirana kontrola pristupa</td></tr>
<tr><td rowspan="2">UTJECAJ MJERA NA RIZIK</td><td colspan="3">Eliminiran rizik</td><td colspan="3">Smanjen rizik</td><td colspan="3">Prihvaćen rizik</td></tr>
<tr><td colspan="3"></td><td colspan="3">X</td><td colspan="3"></td></tr>
</table>

4.3. Povreda (prijenos ili uništenje) osobnih podataka od strane NEovlaštenih osoba

<table>
<tr><td>NAZIV RIZIKA</td><td colspan="10">Povreda (prijenos ili uništenje) osobnih podataka od strane NEovlaštenih osoba</td></tr>
<tr><td>OPIS PRIJETNJE / RIZIKA</td><td colspan="10">dostupnost osobnih podataka zbog neadekvatnih tehničko-sigurnosnih mjera
neovlaštena izmjena ili prijenos osobnih podataka zbog neadekvatnih sigurnosnih mjera
odavanje osobnih podataka zbog neadekvatne kontrole pristupa</td></tr>
<tr><td>IZBJEGAVANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRENOŠENJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRIHVAĆANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>SMANJENJE / UBLAŽAVANJE RIZIKA</td><td colspan="10">Zabranjen pristup neovlaštenim osobama dokumentaciji i IT opremi
Odlaganje papirne dokumentacije u zaključane ormare i ladice
Smještaj IT opreme i arhive u zaštićene prostorije s ograničenim pristupom
Politika 'čistog stola' – smanjenje papirnih dokumenata iz kojih su vidljivi podaci – gostima
Monitor okrenut u smjeru da vanjski suradnik ili gost ne može vidjeti podatke
Korištenje lozinki
Ne davanje vlastite lozinke drugim zaposlenicima
Educiranje zaposlenika i rad na integritetu djelatnika
Kontinuirana pohrana sigurnosnih kopija
Ograničen broj osoba s pravom pristupa</td></tr>
<tr><td rowspan="3">IZVOR/UZROK PRIJETNJE</td><td colspan="9">PRIRODNI</td><td></td></tr>
<tr><td colspan="9">TEHNIČKI – kvar opreme</td><td>X</td></tr>
<tr><td colspan="9">LJUDSKI FAKTOR – unutarnji i vanjski</td><td>X</td></tr>
<tr><td>POSTOJEĆE MJERE ZA SMANJENJE RIZIKA</td><td colspan="10">PREVENTIVNA KONTROLA
Izlazak iz programa nakon prestanka rada –
druga osoba koristi program pod tuđom lozinkom; narušena povjerljivost i integritet)

DETEKTIVNA KONTROLA
Kontrola pohrane sigurnosnih kopija
Promjene lozinki</td></tr>
<tr><td rowspan="2">PROCJENA RAZINE RIZIKA</td><td colspan="3">Vjerojatnost</td><td colspan="3">Učinak</td><td colspan="3">Rizik</td></tr>
<tr><td>Malo vjerojatno</td><td>Vjerojatno</td><td>Vrlo vjerojatno</td><td>Niski utjecaj</td><td>Značajan utjecaj</td><td>Visok utjecaj</td><td>Niski</td><td>Srednji</td><td>Visok</td></tr>
<tr><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>MJERE KOJE ĆE SE PODUZETI ZA SMANJENJE RIZIKA</td><td colspan="10">Potpisana izjava o povjerljivosti
Disciplinski postupak za kršenje sigurnosti -obavještavanje vlasnika o nastalom incidentu
Implementirana kontrola pristupa</td></tr>
<tr><td rowspan="2">UTJECAJ MJERA NA RIZIK</td><td colspan="3">Eliminiran rizik</td><td colspan="3">Smanjen rizik</td><td colspan="3">Prihvaćen rizik</td></tr>
<tr><td></td><td></td><td></td><td></td><td>X</td><td></td><td></td><td></td><td></td></tr>
</table>

4.4. Gubitak osobnih podataka

NAZIV RIZIKA	**Gubitak osobnih podataka**								
OPIS PRIJETNJE / RIZIKA	Kvar IT opreme Elementarna nepogoda – požar, poplava, udar groma								
IZBJEGAVANJE RIZIKA									
PRENOŠENJE RIZIKA									
PRIHVAĆANJE RIZIKA									
SMANJENJE / UBLAŽAVANJE RIZIKA	Smještaj IT opreme i arhive u zaštićene prostorije s ograničenim pristupom. Usluge podrške zaštita od požara, klimatizacija U prostoriji se ne smiju nalaziti izvori čestica prašine, lakozapaljivih sredstava ili tekućina, električnih ili magnetskih polja, te vode. Sigurnost kablova Održavanje opreme Sigurno odlaganje i ponovna uporaba opreme Educiranje zaposlenika Kontinuirana pohrana sigurnosnih kopija								
IZVOR/UZROK PRIJETNJE	PRIRODNI								X
	TEHNIČKI – kvar opreme								X
	LJUDSKI FAKTOR – unutarnji i vanjski								
POSTOJEĆE MJERE ZA SMANJENJE RIZIKA	<u>PREVENTIVNA KONTROLA</u> Postojanje aparata za gašenje požara uz upute za uporabu u neposrednoj blizini arhive i IT opreme. Redovito održavanje opreme / servis <u>DETEKTIVNA KONTROLA</u> Kontrola pohrane sigurnosnih kopija								
PROCJENA RAZINE RIZIKA	Vjerojatnost			Učinak			Rizik		
	Malo vjerojatno	Vjerojatno	Vrlo vjerojatno	Niski utjecaj	Značajan utjecaj	Visok utjecaj	Niski	Srednji	Visok
	X			X			X		
MJERE KOJE ĆE SE PODUZETI ZA SMANJENJE RIZIKA	redovan servis računala redovan servis aparata za gašenje								
UTJECAJ MJERA NA RIZIK	Eliminiran rizik			Smanjen rizik			Prihvaćen rizik		
				X					

4.5. Neovlašteni pristup osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani

<table>
<tr><td>NAZIV RIZIKA</td><td colspan="10">Neovlašteni pristup osobnim podacima koji su preneseni,
pohranjeni ili na drugi način obrađivani</td></tr>
<tr><td>OPIS PRIJETNJE / RIZIKA</td><td colspan="10">Nehotično slanje osjetljivih podataka na krive adrese e-Mail
Neovlašten pristup podacima putem interneta/ mreže od strane hackera
Otvorenost prema malicioznom softveru (virusi, trojanci, crvi…)
Pristup podacima vanjskog suradnika / gosta
Pristup podacima neovlaštenog djelatnika
Upadi u komunikaciju i uništenje poruka</td></tr>
<tr><td>IZBJEGAVANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRENOŠENJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>PRIHVAĆANJE RIZIKA</td><td colspan="10"></td></tr>
<tr><td>SMANJENJE / UBLAŽAVANJE RIZIKA</td><td colspan="10">Korištenje lozinki
Ne davanje vlastite lozinke drugim zaposlenicima
Educiranje zaposlenika i rad na integritetu djelatnika
Kontinuirana pohrana sigurnosnih kopija
Ograničen broj osoba s pravom pristupa
Monitor okrenut u smjeru da vanjski suradnik ili gost ne može vidjeti podatke
Wi-Fi mreža zaštićena lozinkom
Korištenje lozinki</td></tr>
<tr><td rowspan="3">IZVOR/UZROK PRIJETNJE</td><td colspan="9">PRIRODNI</td><td></td></tr>
<tr><td colspan="9">TEHNIČKI – kvar opreme</td><td>X</td></tr>
<tr><td colspan="9">LJUDSKI FAKTOR – unutarnji i vanjski</td><td>X</td></tr>
<tr><td>POSTOJEĆE MJERE ZA SMANJENJE RIZIKA</td><td colspan="10"><u>PREVENTIVNA KONTROLA</u>
Kontrola protiv malicioznog koda (anti virus)
<u>DETEKTIVNA KONTROLA</u>
Kontrola pohrane sigurnosnih kopija</td></tr>
<tr><td rowspan="2">PROCJENA RAZINE RIZIKA</td><td colspan="3">Vjerojatnost</td><td colspan="3">Učinak</td><td colspan="3">Rizik</td></tr>
<tr><td>Malo vjerojatno</td><td>Vjerojatno</td><td>Vrlo vjerojatno</td><td>Niski utjecaj</td><td>Značajan utjecaj</td><td>Visok utjecaj</td><td>Niski</td><td>Srednji</td><td>Visok</td></tr>
<tr><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td>MJERE KOJE ĆE SE PODUZETI ZA SMANJENJE RIZIKA</td><td colspan="10">redovan update antivirusnog programa
Mreža / IT oprema zaštićena vatrenim zidom</td></tr>
<tr><td rowspan="2">UTJECAJ MJERA NA RIZIK</td><td colspan="3">Eliminiran rizik</td><td colspan="3">Smanjen rizik</td><td colspan="3">Prihvaćen rizik</td></tr>
<tr><td colspan="3"></td><td colspan="3">X</td><td colspan="3"></td></tr>
</table>

5. Identifikacija rizika sigurnosti osobnih podataka

Prilikom procjene rizika za sigurnost podataka u obzir se uzimaju rizici koje predstavlja obrada osobnih podataka

Voditelj obrade u dokumentu Politika privatnosti pod točkom ORGANIZACIJSKE I TEHNIČKE MJERE ZAŠTITE OSOBNIH PODATAKA određuje fizičke, tehničke i organizacijske mjere koje su potrebe kako bi se rizik kod obrade osobnih podataka umanjio, što osobito može dovesti do smanjenja materijalne ili nematerijalne štete.

Rizici koje predstavlja obrada osobnih podataka	*Vrsta rizika*
Krađa osobnih podataka unutar/izvan organizacije	Mali rizik
Povreda osobnih podataka od strane ovlaštenih osoba	Mali rizik
Povreda (prijenos ili uništenje) osobnih podataka od strane NEovlaštenih osoba	Mali rizik
Gubitak osobnih podataka	Mali rizik
Neovlašteni pristup osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani	Mali rizik