Dječji vrtić Loptica
Tina Ujevića 12
40000 Čakovec
OIB:75764016426
Tel: 040 384 066
djecji.vrtic.loptica@gmail.com

GDPR-SIGURNOST PODATAKA

Pravilnik o sigurnosti osobnih podataka

KLASA: _____

BROJ: _____

	Ime i prezime, funkcija	**Datum**	**Potpis:**
Izradio:	**Dječji vrtić Loptica**	19.01.2021.	
Odobrio:	**Dječji vrtić Loptica -**ravnateljica	19.01.2021.	

SADRŽAJ

1. UVOD

1.1. Područje primjene

Ovim pravilnikom definiraju se pravila za zaštitu 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).

Voditelj obrade djeluje na sljedećim lokacijama
1. Dječji vrtić Loptica - Čakovec
2. Područni odjel Medo – Orehovica

Kako bi zaštitili osobne podatke koje prikuplja, Voditelj obrade provodi odgovarajuće fizičke, tehničke i organizacijske mjere zaštite, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode ispitanika za osiguravanje usklađenosti s Općom uredbom o zaštiti osobnih podataka Članak 25 i Članak 32.
To se prije svega odnosi na prevenciju povreda osobnih podataka poput gubitka ili oštećenja, nedopuštenog pristupa, mijenjanja ili obrade podataka ili bilo kojeg drugog rizika kojem podaci mogu biti izloženi. Usvajanjem ove politike također znači da će ukoliko dođe do ugrožavanja prava i sloboda ispitanika na privatnost, nastala šteta biti reducirana u kojoj mjeri je to moguće

Politikom privatnosti osigurava se adekvatna razina zaštite podataka u skladu s Općom uredbom o zaštiti podataka i drugim primjenjivim važećim zakonima vezanim uz zaštitu osobnih podataka.

2. MJERE ZAŠTITE OSOBNIH PODATAKA

To se prije svega odnosi na prevenciju povreda osobnih podataka poput gubitka ili oštećenja, nedopuštenog pristupa, mijenjanja ili obrade podataka ili bilo kojeg drugog rizika kojem podaci mogu biti izloženi. Usvajanjem ove politike također znači da će ukoliko dođe do ugrožavanja prava i sloboda ispitanika na privatnost, nastala šteta biti reducirana u kojoj mjeri je to moguće

Osnovni ciljevi sigurnosnih mjera
- Sprečavanje pristupa obrade osobnih podataka neovlaštenim osobama
- Očuvanje sigurnosti osobnih podataka koji se čuvaju ili prenose kako ne bi mogli biti kopirani ili pročitani, modificirani ii uklonjeni bez odobrenja
- Osiguranje zaštite osobnih podataka protiv neželjenog uništavanja ili gubitka
- Čuvanje osobnih podataka samo onoliko dugo koliko je nužno i potrebno

Kršenje ove politike i ugrožavanje osobnih podataka može rezultirati sankcijama koje određuje voditelj obrade a u nekim slučajevima može imati i pravne posljedice

Kako bi se pojačao nadzor nad aktivnostima obrade osobnih podataka, voditelj obrade i ispitanik u svakom će trenutku biti svjesni svrha i postupaka koji se primjenjuju. Podaci će se prikupljati na temelju jasno definirane pravne osnove kako bi se osigurala legitimnost obrade, pri ćemo će o tome u svakom primjenjivom slučaju ispitanik biti informiran. Na taj se način ispitaniku jamči transparentnost i pravedno ophođenje pri obradi podataka. Podaci koji su prikupljeni za određenu svrhu neće se koristiti ni za koju drugu svrhu osim navedene. Ukoliko je potrebno proširiti svrhu obrade voditelj obrade će o tome svakako obavijestiti ispitanika.

Osnovni podaci neće se čuvati u obliku koji omogućava identifikaciju ispitanika dulje no što je potrebno za svrhu obrade. Također, rok čuvanja bit će jasno određen i ograničen na vrijeme koje je nužno za ostvarivanje svrhe obrade i čuvanja osobnih podataka. Nakon isteka roka čuvanja, podaci će biti uklonjeni ili anonimizirani i obrada prekinuta

Zaštita osobnih podataka temelji se na svijesti o njihovu korištenju, što znači da će voditelj obrade voditi računa ne samo o vlastitom poznavanju donesenih procedura, već i o edukaciji te upoznavanju svojih zaposlenika i suradnika s odredbama Uredbe i internih politika.
Vodit će se evidencija o obrazovanju kojom će se dokazati aktivna primjena ove politike i ažurnost u ostvarivanju cilja zaštite osobnih podataka.

2.1. Fizičke mjere zaštite

Voditelj obrade propisuje sljedeće mjere fizičke zaštite:

(a) Minimalne fizičke mjere zaštite postupanja s papirnom dokumentacijom sa sadržanim osobnim podacima odnose se na odlaganje papirnate dokumentacije u zaključane ormare i ladice, iz razloga što osobni podaci moraju biti fizički nedostupni svim osobama koje im nemaju pristup.
(b) Minimalne fizičke mjere zaštite prostorije u kojoj se pohranjuje IT oprema koju je potrebno osigurati odnosi se na smještaj IT opreme u zaštićene prostorije s ograničenim pristupom, postojanje aparata za gašenje požara uz upute za uporabu u neposrednoj blizini prostorije. U prostoriji se ne smiju nalaziti izvori čestica prašine, lakozapaljivih sredstava ili tekućina, električnih ili magnetskih polja, te vode.
(c) pohranjivanje USB prijenosnih memorija u zaključani ormar ili ladicu,

2.2. Tehničke mjere zaštite

2.2.1. Pohrana sigurnosnih kopija

Na sigurnosne kopije, jednako kao i na samu bazu u kojoj se nalaze osobni podaci, primjenjuju se iste tehničke mjere zaštite kao što su da kopija baze mora biti zaštićena najmanje kao original, da lokacija za pohranu sigurnosnih kopija mora biti zaštićena od neovlaštenog pristupa, da se arhiva kreira preslikama isprava ili elektroničkim zapisom.
Osnovna strategija izrade sigurnosnih kopija odnosi se na drugi sigurnosni uređaj i na One drive - cloud servis. Kopije podataka iz knjigovodstvenog programa (izdavanje ponuda, računa) pohranjuju se automatski na server IT administratora, kopije podataka sa osobnih računala se izrađuju prema potrebi odnosno najkasnije u 5 radnih dana na drugi sigurnosni uređaj ili na One drive - cloud servis.

2.2.2. Antivirusna zaštita

Na serveru i svim računalima koji pristupaju mreži Voditelj obrade moraju imati instaliranu antivirusnu zaštitu (program) u skladu s najvišim standardima zaštite koji se redovito obnavlja.
Ovo pravilo se odnosi i na prijenosna računala koja se redovito povezuju s mrežom Voditelj obrade.
Voditelj obrade kao dokaz instaliranih programa antivirusne zaštite vodi evidencije instaliranih antivirusnih programa i evidentira informacije o programu i licenci i datum isteka korištenja.
Svi instalirani antivirusni programi trebaju imati uključeno automatsko ažuriranje.
Svi radnici koji u radu koriste računala upoznati su sa osnovama sigurnog rada na računalima, obvezom da se ne otvaraju e-mail poruke nepoznatih pošiljatelja i sumnjivog sadržaja, i obvezom da se koristi samo licencirani softver koji odobri nadležna osoba Voditelja obrade.

2.2.3. Korištenje lozinki

Sustavi (računala i prijenosna računala) koji obrađuju osobne podatke trebaju biti zaštićeni kontrolom pristupa koji se temelji na lozinki. Lozinke moraju biti sastavljene od kombinacije slova, brojeva i posebnih znakova (interpunkcijskih oznaka i simbola). Lozinke moraju imati kombinaciju velikih i malih slova.
Lozinke ne bi trebale sadržavati očiti slijed znakova na tipkovnici (npr qwertz ili 12345). Ne preporuča se korištenje iste lozinke za pristup različitim sustavima.

Nadređene osobe nisu ovlašteni tražiti, prikupljati i pohranjivati lozinke zaposlenika. Dozvoljeno je korištenje zajedničke lozinke za više djelatnika, ako je to poslovno opravdano.

Strogo je zabranjeno dijeljenje lozinki. Lozinke se ne smiju otkrivati ili javno prikazivati. Zabranjeno je slanje lozinki elektroničkom poštom. Uvijek kada se lozinka smatra kompromitiranom, odmah se mora promijeniti.

2.3. Organizacijske mjere zaštite

2.3.1. Dodjela ovlaštenja sukladno radnom mjestu

Voditelj obrade u skladu s radnim mjestom definira osobe kojima dodjeljuje posebna ovlaštenja za određene poslove i zadatke što se odnosi na sljedeće: pohranjivanje, obrada i prijenos osobnih podataka, kako bi se samo toj osobi dozvolio pristup u prostorije ili pristup ključevima od ormara i ladica u kojima se nalaze osobni podaci, poslove pohrane sigurnosnih kopija, te odrediti ovlasti i detaljan plan izrade sigurnosnih kopija.

Voditelj obrade djelatnicima koji provode obradu osobnih podataka ili na koji drugi način dolaze do osobnih podataka unutar tvrtke daje na potpis Izjavu o provjerljivosti (Kadrovska usklađenost) kako bi zajamčilo da neće ustupati, pokazivati ili na bilo koji drugi način davati na uvid sadržaj osobnih podataka nikome osim ovlaštenim primateljima, koja se nalazi u prilogu Politike i smatra se njezinim sastavnim dijelom.

2.4. Korištenje informatičke opreme

Sva informatička oprema može se koristiti isključivo u poslovnim aktivnostima za koje je namijenjena. Svaki korisnik je odgovoran za očuvanje i ispravnu upotrebu informatičke opreme koja mu je dana na korištenje. Sva informatička oprema mora biti na mjestima s kontroliranim pristupom.

Aktivna radna površina i prijenosna računala moraju biti osigurana ukoliko nisu pod nadzorom. Kada je god moguće, spomenuto pravilo mora se provoditi automatski.

Pristup infrastrukturi nije dozvoljen neovlaštenim osobama. Dodjeljivanje pristupa informatičkoj infrastrukturi i računalnim mrežama mora se obaviti putem odobrenih i prihvaćenih postupaka za upravljanje uslugama informatičke infrastrukture i nadziranim upravljanjem pristupom.
Korisnici se moraju prema opremi, koja im je povjerena na korištenje, odnositi s punom pažnjom, te s njom pažljivo rukovati te izbjegavati nepravilno korištenje.
Posebna se pažnja mora posvetiti zaštiti prijenosnih računala, tableta, pametnih telefona i drugih prijenosnih uređaja od krađe ili gubitka.
Također, u obzir treba uzeti druge rizike oštećenja infrastrukture te oštećenja koji mogu rezultirati povredom ili gubitkom podataka kao što su ekstremne temperature, magnetska polja ili padovi.
Uvijek kada je moguće, neophodno je koristiti tehnologiju šifriranja i brisanja u slučaju gubitka ili krađe prijenosne infrastrukture.

Gubitak, krađa, oštećenje, neovlašteno korištenje ili drugi incidenti moraju se, što prije od trenutka spoznaje, prijaviti odgovornoj osobi.
Zbrinjavanje imovine koja se više ne koristi mora se izvršiti u skladu s posebnim postupcima zbrinjavanja informatičkog otpada, uzimajući u obzir zaštitu svih informacija koji su predmet takvog oblika obrade. Imovina koja pohranjuje povjerljive podatke mora biti uništena u prisustvu odgovorne osobe. Sredstva za čuvanje osjetljivih informacija moraju se prije odlaganja u potpunosti izbrisati u nazočnosti odgovorne osobe.

2.4.1. Sigurnost korištenja informacijskih i komunikacijskih uređaja

Kako bi se spriječio neovlašteni pristup podacima u uređaju i ostalim podacima kojima uređaj ima pristup, uređaj mora biti zaštićen lozinkom.
Ukoliko postoji opcija kriptiranja uređaja, uređaj mora biti kriptiran. Pristup mreži s uređaja također mora biti zaštićen lozinkom s isključenom opcijom automatskog prepoznavanja mreže.

Gubitak ili krađa uređaja mora se prijaviti nadležnoj osobi voditelja obrade, najkasnije 24 sata od spoznaje o gubitku ili krađi. Zaposlenici su odgovori za obavješćivanje mobilnog operatera o krađi ili gubitku odmah nakon gubitka ili krađe uređaja.
Očekuje se da će svaki zaposlenik u svakom trenutku koristiti svoje uređaje na etičan način u skladu s pravilima tvrtke i etičkim kodeksom.
Zaposlenik preuzima punu odgovornost za rizike djelomičnog ili potpunog gubitka podataka pohranjenih na uređaju zbog nepravilnog korištenja ili grešaka koje uređaj čine neupotrebljivim.

2.4.2. Mrežne mjere zaštite i korištenje interneta

Pravila korištenja interneta i elektroničke pošte odnose se na sve korisnike interneta. Za sve korisnike interneta dopušten je ograničen pristup. Strogo je zabranjen pristup pornografskim web stranicama i svim drugim rizičnim stranicama.
Pristup internetu uglavnom je predviđen za poslovnu namjenu. Pristup internetu u osobne svrhe je dopušten uz uvjet da se ne utječe na produktivnost rada.
Obeshrabruje se korištenje interneta za osobne svrhe tijekom radnog vremena. Pri pristupanju internetu, korisnici se moraju ponašati u skladu s pravilima koja osiguravaju ugled. Potrebno je poduzeti razumne mjere za otkrivanje i sprečavanje napada na servere i radne stanice

3. ZAVRŠNE ODREDBE

Ovaj Pravilnik o SIGURNOST OSOBNIH PODATAKA stupa na snagu danom donošenja i bit će objavljen na oglasnoj ploči Voditelja obrade.

4. POVIJEST VERZIJA

POVIJEST VERZIJA				
Verzija	Datum	Izradio	Odobrio	Opis
1.0	31.12.2019.	Dječji vrtić Loptica	Dječji vrtić Loptica	
2.0	19.01.2021		Dječji vrtić Loptica	Ažuriranje dokumenta – smanjenje broja lokacija

5. PRILOZI

5.1. Izjava o povjerljivosti

Ovom izjavom obvezujem se da ću sukladno propisima koji uređuju područje zaštite osobnih podataka, Uredbom (EU) 2016/679 europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka, čuvati povjerljivost svih osobnih podataka kojima imam pravo i ovlast pristupa, a koji se nalaze u sustavima pohrane koje vodi tvrtka u kojoj sam zaposlen/a te da ću iste osobne podatke koristiti isključivo u točno određenu / propisanu svrhu koja je opisana u Internim aktima koje donosi poslodavac, a odnose na usklađenje sa predmetnom regulativom - Politika privatnosti.

Također se obvezujem da osobne podatke kojima imam pravo i ovlast pristupa neću dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnima trećim (neovlaštenim) osobama, te se obvezujem da ću povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima.

Upoznat/a sam da bilo kakvo neovlašteno raspolaganje osobnim podacima kojima imam pravo pristupa u svojem radu predstavlja povredu radne obveze kod voditelja obrade.

Datum: _____

Ime i prezime: _____

Potpis: _____