KANTONALNO JAVNO KOMUNALNO PREDUZEĆE
"VODOVOD I KANALIZACIJA" d.o.o. SARAJEVO
PREDUZEĆE ZA PROIZVODNJU I DISTRIBUCIJU VODE, ODVOĐENJE I PREČIŠĆAVANJE OTPADNIH VODA
Por. br.: 01841358, Mat. br.: 20187646, Općinski sud u Sarajevu, rješenje broj: 065-0-Reg-21-005229
Sjedište: ul. Jaroslava Černija br. 8, tel: 033/237-655, 033/483-400, fax: 033/440-658, www.viksa.ba
e-mail: press@viksa.ba PDV-IB: 200151950004, ID: 4200151950004

PLAN SIGURNOSTI LIČNIH PODATAKA
KJKP „VODOVOD I KANALIZACIJA“ D.O.O. SARAJEVO

SARAJEVO, maj. 2026. Godine

Na osnovu člana 26. Zakona o zaštiti ličnih podataka ("Službeni glasnik BiH", broj: 12/25), člana 89. stav (5) Statuta KJKP "Vodovod i kanalizacija" d.o.o. Sarajevo broj: 2317/22 od 18.04.2022. godine te člana 20. Pravilnika o provođenju odredaba Zakona o zaštiti ličnih podataka u KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo broj 2V-04/26 od 28.01.2026 godine, Uprava Preduzeća JE na 50. sjednici održanoj dana 18.05.2026. godine donijela:

PLAN SIGURNOSTI LIČNIH PODATAKA KJKP „VODOVOD I KANALIZACIJA" D.O.O. SARAJEVO

I - OPĆE ODREDBE

Član 1.
(Predmet)

Planom sigurnosti ličnih podataka (u daljem tekstu: Plan) utvrđuju se ciljevi, organizacijske i tehničke i mjere kojima se osigurava zaštita ličnih podataka čiju obradu u okviru svojih nadležnosti vrši KJKP "Vodovod i kanalizacija" d.o.o. Sarajevo (u daljem tekstu: Preduzeće).

Član 2.
(Definicije pojmova)

a) *"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)
b) *"povreda ličnog podatka"* je kršenje bezbjednosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlašćenog otkrivanja ili pristupa ličnim podacima koji su preneseni, čuvani ili na drugi način obrađivani,
c) *"nosilac podataka"* je fizičko lice čiji je identitet utvrđen ili čiji se identitet može utvrditi, posredno ili neposredno, posebno pomoću identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili pomoću jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog lica,
d) "k*ontrolor podataka*" je fizičko ili pravno lice, javni organ ili nadležni organ koji samostalno ili s drugim određuje svrhe i sredstva obrade ličnih podataka,
e) "*obrađivač*" je fizičko ili pravno lice, javni organ koji obrađuje lične podatke u ime kontrolora podataka,
f) "*primalac*" je fizičko ili pravno lice, javni organ kojem se otkrivaju lični podaci, nezavisno od toga da li je u pitanju treća strana. Javni organi koji mogu primiti lične podatke u okviru određene istrage u skladu sa zakonom ne smatraju se primaocima, ali obrada tih podataka mora biti u skladu sa važećim pravilima o zaštiti podataka prema svrhama obrade,
g) *"obrada"* je svaki postupak ili skup postupaka koji se obavlja na ličnim podacima ili na skupovima ličnih podataka, automatizovanim ili neautomatizovanim sredstvima, kao što su prikupljanje, evidentiranje, organizacija, strukturiranje, čuvanje, prilagođavanje ili izmjena, pronalaženje, ostvarivanje uvida, upotreba, otkrivanje prenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombinovanje, ograničenje, brisanje ili uništavanje,
h) *"ograničenje obrade"* je obilježavanje čuvanog ličnog podatka s ciljem ograničenja njegove obrade u budućnosti,
i) *„anonimizacija"*primjenjivaće se u slučajevima kada podaci više nisu potrebni za identifikaciju pojedinca, a zadržavaju se isključivo u statističke, analitičke, izvještajne ili istraživačke svrhe. Anonimizirani podaci obrađuju se na način kojim se trajno i nepovratno onemogućava identifikacija nosioca podataka, te se takvi podaci više ne smatraju ličnim podacima u smislu važećeg zakona.

j) *"pseudonimizacija"* je obrada ličnog podatka tako da se lični podatak više ne može pripisati određenom nosiocu podataka bez korištenja dodatnih informacija, uz uslov da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacionim mjerama kako bi se osiguralo da se lični podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi,

k) *"zbirka ličnih podataka"* je svaki strukturirani skup ličnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to da li su centralizirani, decentralizirani ili rasprostranjeni na funkcionalnoj ili geografskoj osnovi,

l) *"saglasnost nosioca podataka"* je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje nosioca podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu ličnih podataka koji se na njega odnose.

m) *"genetski podatak"* je lični podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičkog lica koja daju jedinstvene informacije o fiziologiji ili zdravlju tog fizičkog lica i koji su dobiveni posebnom analizom biološkog uzorka tog fizičkog lica;

n) *"biometrijski podatak"* je lični podatak dobiven posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičkog lica koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica, kao što su fotografije lica ili daktiloskopski podaci.

Član 3.

(Zakonitost)

Obrada ličnih podataka vrši se u skladu sa Zakonom o zaštiti ličnih podataka ("Službeni glasnik BiH", broj: 12/25 od 28.02.2025. godine), Pravilnikom o provođenju odredaba Zakona o zaštiti ličnih podataka u KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo broj 2V-04/26 od 28.01.2026 godine, kao i drugim važećim propisima koji uređuju oblast zaštite ličnih podataka, a zasniva se na legitimnom interesu, saglasnosti nosioca podataka i/ili izvršenju ugovornih obaveza.

Član 4.

(Primjena)

(1) Ovaj Plan se primjenjuje na sve organizacione jedinice Preduzeća, kao i na sva lica koja po bilo kojem osnovu postupaju po ovlaštenju Preduzeća kao kontrolora ličnih podataka, uključujući zaposlene, angažovana lica, vanjske obrađivače i pružaoce usluga.

(2) Plan se primjenjuje na sve sisteme, evidencije i procese koji uključuju automatizovanu i neautomatizovanu obradu ličnih podataka, u skladu sa Zakonom o zaštiti ličnih podataka u Bosni i Hercegovini i relevantnim podzakonskim aktima.

Član 5.

(Odgovornost i ovlaštenja)

(1) Planom se utvrđuju odgovornosti, ovlaštenja i mjere zaštite kojima se obezbjeđuju povjerljivost, integritet i raspoloživost sistema u kojima se obrađuju lični podaci, identifikuju se korisnici koji su odgovorni za praćenje i provođenje Plana unutar svojih područja odgovornosti i vrsta informacija kojih su oni vlasnici, a koji se smatraju posebno osjetljivim, odnosno povjerljivim.

(2) U okviru sistema zaštite ličnih podataka, jasno su definisane uloge i odgovornosti svih učesnika u procesu obrade, kako bi se obezbijedila zakonitost, sigurnost i povjerljivost podataka:

a) Preduzeće kao Kontrolor podataka odgovorno je za zakonitost obrade i sporovođenje mjera zaštite,

b) Službenik za zaštitu ličnih podataka vrši nadzor nad primjenom propisa, vrši edukaciju zaposlenih, komunicira sa Agencijom za zaštitu ličnih podataka u BiH, djeluje nezavisno, pruža savjete u vezi sa obavezama iz Zakona, prati primjenu propisa, učestvuje u procjenama uticaja na zaštitu podataka.

c) Zaposleni koji obrađuju lične podatke dužni su čuvati povjerljivost ličnih podataka kojima pristupaju u okviru posla,
d) Obrađivači podataka postupaju po uputstvima kontrolora i primjenjuju tehničke i organizacione mjere zaštite.

(3) Preduzeće je odgovorno za uspostavljanje, primjenu i dokumentovanje tehničkih i organizacionih mjera zaštite ličnih podataka, kao i za dokazivanje usklađenosti obrade sa Zakonom.

Član 6.
(Ciljevi)

Cilj Plana je osigurati:

- zakonitu, poštenu i transparentnu obradu ličnih podataka,
- obradu podataka u skladu sa načelima ograničenja svrhe, minimizacije podataka i ograničenja čuvanja,
- tačnost i ažurnost ličnih podataka,
- zaštitu ličnih podataka od neovlaštenog ili nezakonitog pristupa, gubitka, izmjene, otkrivanja ili uništenja,
- ostvarivanje i zaštitu prava nosilaca podataka,
- uspostavljanje sistema odgovornosti i dokazivanja usklađenosti obrade sa Zakonom.

Član 7.
(Povjerljivost)

(1) Radnici Preduzeća mogu imati uvid u lične podatke koji se obrađuju, samo ukoliko iz opisa radnog mjesta na koje su raspoređeni proizilazi potreba pristupa ličnim podacima, odnosno evidencijama ličnih podataka koji se obrađuju u Preduzeću, te ako posjeduju korisničko ime i pristupnu šifru dodjeljenu na način i po postupku koji je propisan ovim Planom, a u skladu sa Opštim uputstvom za šifriranje u Preduzeću.

(2) Izuzetno, radnicima Preduzeća može biti omogućen pristup ličnim podacima iako takav pristup ne proizilazi iz opisa radnog mjesta na koje su raspoređeni, ukoliko za tim postoji opravdana potreba u vezi sa obavljanjem radnih zadataka.

(3) U slučaju iz stava (2) ovog člana, radnici moraju imati posebno ovlaštenje direktora Preduzeća ili lica koje direktor ovlasti.

(4) Odobrenje iz stava (3) ovog člana mora sadržavati jasnu naznaku koji podaci odnosno zbirke ličnih podataka se mogu obrađivati.

(5) Radnicima iz stava (2) ovoga člana će se dodijeliti pristupno korisničko ime i šifra koji će važiti samo za određeni period naznačen u odobrenju iz stava (3) ovog člana.

(6) Izvršioci su odgovorni za čuvanje zbirki ličnih podataka u smislu sprečavanja neovlaštenog pristupa i korištenja, kao i tačnost i autentičnost podataka unesenih u zbirke.

(7) Svi radnici koji u svom radu prikupljaju i obrađuju lične podatke dužni su potpisati Izjavu o povjerljivosti i čuvanju ličnih podataka, koja se nalazi u prilogu Pravilnika o provođenju odredaba Zakona o zaštiti ličnih podataka u KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo (Prilog 1.).

(8) U slučaju da zaposleni odbije potpisati Izjavu o povjerljivosti nadležni rukovodioci su obavezni onemogućiti pristup ličnim podacima, kao i obavljanje poslova koji uključuju obradu istih, a takvo postupanje može predstavljati osnov za preduzimanje mjera u skladu sa važećim propisima i internim aktima Preduzeća.

Član 8.
(Integritet)

(1) Radnici koji obrađuju lične podatke dužni su osigurati da su lični podaci tačni i ažurni, te ih pravovremeno ažurirati na osnovu relevantne dokumentacije.

(2) Ukoliko postoji potreba za izmjenom ili dopunom evidencija o aktivnostima obrade ličnih podataka, izvršioci obrade dužni su bez odlaganja obavijestiti Službenika za zaštitu ličnih podataka o potrebi ažuriranja podataka u evidencijama koje se vode u okviru Preduzeća, u skladu sa Zakonom o zaštiti ličnih podataka i Pravilnikom o provođenju Zakona o zaštiti ličnih podataka u KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo, uz obavezno navođenje odgovarajućeg pravnog osnova obrade.

(3) Nakon zaprimanja prijedloga, Službenik za zaštitu ličnih podataka pokreće postupak ažuriranja Evidencije o aktivnostima obrade, koji odobrava Uprava Preduzeća.

Član 9.
(Raspoloživost)

(1) Radnici Preduzeća dužni su podatke iz zbirke ličnih podataka koje obrađuju činiti dostupnim i na raspolaganju licima koja imaju ovlaštenje za uvid.

(2) Radnici iz prethodnog stava mogu podatke iz zbirke ličnih podataka dostavljati drugim organizacionim jedinicama Preduzeća, radnicima Preduzeća i licima van Preduzeća isključivo u obimu koji je neophodan za ostvarivanje njihovih ovlaštenja i radnih zadataka, i samo ako za takvo davanje postoji važeći pravni osnov u skladu sa Zakonom. Svako postupanje s podacima mora biti u skladu sa propisanim mjerama zaštite, načelima obrade i internim aktima Preduzeća.

Član 10.
(Autentičnost)

(1) Radnici koji obrađuju lične podatke dužni su voditi računa o porijeklu ličnih podataka.

(2) Lični podaci mogu biti prikupljeni iz sljedećih izvora:

- neposredno od nosioca podataka, uz prethodno pruženu informaciju o svrsi i pravnom osnovu obrade;
- preuzimanjem iz drugih zbirki ličnih podataka, uz uslov da za takvo preuzimanje postoji zakonit pravni osnov i da je nosilac podataka o tome informisan, osim ako zakonom nije drugačije propisano;
- od trećeg lica, koje mora biti identifikovano imenom, prezimenom i drugim relevantnim podacima, uz obavezu da daje tačne i zakonito pribavljene podatke, te da je nosilac podataka informisan o izvoru, osim ako to nije dozvoljeno ili je izuzeto posebnim propisima;
- iz drugih izvora navedenih u pojedinačnim zbirkama ličnih podataka, pod uslovom da je prikupljanje u skladu sa propisanom svrhom, obimom obrade i načelima zaštite ličnih podataka.

Član 11.
(Anonimizacija i pseudonimizacija ličnih podataka)

(1) U cilju unapređenja sigurnosti obrade ličnih podataka i smanjenja rizika po prava i slobode nosilaca podataka, Planom sigurnosti predviđa se primjena mjera **anonimizacije i pseudonimizacije** ličnih podataka, u skladu sa Zakonom.

(2) **Anonimizacija** ličnih podataka primjenjivaće se u slučajevima kada podaci više nisu potrebni za identifikaciju pojedinca, a zadržavaju se isključivo u statističke, analitičke, izvještajne ili istraživačke svrhe. Anonimizirani podaci obrađuju se na način kojim se trajno i nepovratno onemogućava identifikacija nosioca podataka, te se takvi podaci više ne smatraju ličnim podacima u smislu važećeg zakona.

(3) **Pseudonimizacija** se primjenjuje kao tehnička i organizaciona mjera zaštite u procesima obrade u kojima je identifikacija lica privremeno ili djelimično potrebna. Lični podaci se obrađuju na način da se ne mogu povezati s određenim licem bez korištenja dodatnih informacija (ključa), koje se

čuvaju odvojeno, uz strogo ograničen pristup i primjenu odgovarajućih tehničkih i organizacionih sigurnosnih mjera.

(4) Primjena mjera anonimizacije i pseudonimizacije doprinosi smanjenju rizika od neovlaštenog pristupa, otkrivanja ili zloupotrebe ličnih podataka, jačanju usklađenosti sa načelima minimizacije podataka, ograničenja svrhe i sigurnosti obrade, povećanju nivoa zaštite ličnih podataka u slučaju sigurnosnih incidenata.

(5) Mjere anonimizacije i pseudonimizacije redovno će se preispitivati i, po potrebi, prilagođavati razvoju tehničkih mogućnosti, prirodi i obimu obrade, kao i rezultatima procjene rizika, uključujući i rezultate procjena uticaja na zaštitu podataka (DPIA), kada su iste primjenjive.

Član 12.

(Kategorije ličnih podataka)

(1) Preduzeće u pisanoj i elektronskoj formi vodi slijedeće zbirke ličnih podataka, u skladu sa Pravilnikom o provođenju Zakona o zaštiti ličnih podataka u KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo:

- Evidencije o bivšim i sadašnjim radnicima u Preduzeću;
- Evidenciji o osobama koje za Preduzeće obavljaju rad a nisu u radnom odnosu (ugovor o djelu, ugovor o obavljanju povremenih i privremenih poslova);
- Evidencije o obračunu i isplatama plaća i drugih naknada;
- Evidencije o obračunu i isplatama naknada članovima organa Preduzeća, komisijama i osobama angažovanim po drugim osnovima;
- Evidencije o utuženim dužnicima koji se odnose na fizička lica iz kategorije Domaćinstva i fizička lica koja obavljaju samostalne djelatnosti;
- Evidencije o kupcima/korisnicima usluga;
- Evidencije o obradi ličnih podataka snimljenih putem sistema video nadzora;
- Evidencije o obradi ličnih podataka snimljenih putem sistema audio zapisa telefonskog razgovora;
- Evidencije o obradi ličnih podataka lica koja posjećuju službene prostorije Preduzeća;
- Evidencije o obradi ličnih podataka radnika koji obavljaju poslove fizičke i tehničke zaštite periodičnoj provjeri korištenja vatrenog oružja, psiho-fizičkoj sposobnosti i stručnoj obuci istih;
- Evidencije o ljekarskim pregledima zaposlenika raspoređenih na radna mjesta sa posebnim uslovima rada;
- Evidencije o kandidatima prijavljenim na Javni oglas za prijem u radni odnos kao i za imenovanja u organe Preduzeća (Uprava, Nadzorni odbor, Skupština, Odbor za reviziju);
- Evidencije o intervencijama kod korisnika usluga;
- Evidencije o obradi ličnih podataka prikupljenih putem web stranice Preduzeća;
- Evidencije o obradi ličnih podataka za potrebe komunikacije s medijima i javnošću;
- Evidencije o obradi ličnih podataka za potrebe online podrške eksternim subjektima;
- Evidencije o obradi ličnih podataka u Odjelu za internu reviziju;
- Evidencije o obradi ličnih podataka na Protokolu Preduzeća;
- Evidencije o obradi ličnih podataka u Arhivi Preduzeća;
- Evidencije o obradi ličnih podataka za korisnike usluga priključenja na vodovodnu i kanalizacionu mrežu;
- Evidencije o obradi ličnih podataka za potrebe provođenja postupka javnih nabavki;
- Evidencije o kontroli nelegalne potrošnje komunalne/vodne usluge (fizička lica iz kategorije „Domaćinstva" i fizička lica koja obavljaju samostalne djelatnosti, ostali korisnici, privredni subjekti),

(2) Vrste i način vođenja zbirki ličnih podataka propisan je Pravilnikom o provođenju zakona o zaštiti ličnih podataka u KJKP „VIK" d.o.o. Sarajevo.

II – ORGANIZACIJSKE MJERE ZAŠTITE LIČNIH PODATAKA

Član 13.
(Definicija)

Organizacijske mjere zaštite ličnih podataka predstavljaju sistem mjera koje obuhvataju jasno definisanje ovlaštenja, obima prava na obradu, uvid i kontrolu ličnih podataka, informisanje i obuku radnika u cilju sprečavanja njihove zloupotrebe.

Član 14.
(Organizacija obrade i postupanje u slučaju povrede ličnih podataka)

Organizacija obrade, svrha i obim, ovlaštenja, kontrola ličnih podataka te postupanje u slučaju povrede ličnih podataka u Preduzeću vrši se na sljedeći način:

a) Evidencija o bivšim i sadašnjim radnicima Preduzeća

Evidencije o ličnim podacima	Evidencija o bivšim i sadašnjim radnicima Preduzeća vodi se u SEPP-u/Služba za pravne poslove i upravljanje ljudskim resursima u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu regulisanja prava i obaveza iz radnog odnosa, ispunjenja zakonskih obaveza Preduzeća, vođenja kadrovske administracije, obračuna plata i drugih opravdanih poslovnih potreba.
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u Službi.
Obim ličnih podataka koji se obrađuju	U evidenciji se obrađuju samo podaci nužni za ostvarivanje svrhe obrade, i to najčešće: identifikacijski podaci (ime, prezime, JMBG, datum i mjesto rođenja), podaci o kontaktu (adresa, telefon, e-mail), podaci o radnom odnosu (radno mjesto, status zaposlenja, vrsta ugovora, staž, radno vrijeme, odmori, invalidnost, učešće u oružanim snagama), podaci o obrazovanju, stručnoj spremi i radnom iskustvu, podaci o obračunu plata i naknada, podaci o ocjenama rada, disciplinskim postupcima, prestanku radnog odnosa, drugi podaci propisani zakonom ili neophodni za zakonito ostvarivanje prava i obaveza iz radnog odnosa.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji/dosijeu imaju isključivo radnici koji su za to ovlašteni u Službi za pravne poslove i upravljanje ljudskim resursima (Referent za upravljanje ljudskim resurima). Svako ovlaštenje utvrđuje se prema radnom mjesu i zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke/dosije zaposlenih ima, Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Referent za upravljanje ljudskim resursima i Izvršni direktor za ekonomske i pravne

	poslove. Uvid u lične podatke može biti omogućen: radnicima na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke evidentiraju se u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u Službi za pravne poslove i upravljanje ljudskim resursima te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku (dosije) čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom; elektronske evidencije se čuvaju u sistemima s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s Listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za pravne poslove i upravljanje ljudskim resursima	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika (osobe koje za Preduzeće obavljaju rad, a nisu u radnom odnosu), službe su dužne preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (službe moraju sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (službe bez odlaganja, a najkasnije u roku od dva sata, obavještavaju Službenika za zaštitu ličnih podataka, putem e-maila ili internog sistema - dostavljaju sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima.

	Procjena rizika (Rukovodilac Službe za pravne poslove i upravljanje ljudskim resursima, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile službe). **Obavještavanje oštećenih radnika** (Ako povreda može uzrokovati štetu radnicima Služba za pravne poslove i upravljanje ljudskim resursima ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

b) **Evidencije o osobama koje za Preduzeće obavljaju rad, a nisu u radnom odnosu (Ugovor o djelu, ugovor o obavljanju povremenih i privremenih poslova)**

Evidencije o ličnim podacima	Evidencija o osobama koje za Preduzeće obavljaju rad, a nisu u radnom odnosu (Ugovor o djelu, ugovor o obavljanju povremenih i privremenih poslova) vodi se u SEPP-u/Službi za pravne poslove i upravljanje ljudskim resursima i Službi za računovodstvo i finansije u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu ostvarivanja prava, a na osnovu važećih zakonskih i podzakonskih propisa, te drugih općih akata koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	U evidenciji se obrađuju samo podaci nužni za ostvarivanje svrhe obrade, i to najčešće: ime i prezime, broj telefona, broj lične karte, organ koji je izdao i mjesto izdavanja, JMBG, adresa stanovanja, učešće u oružanim snagama, invalidnost, općina stanovanja, transakcijski račun i banka kod koje se vodi isti, podaci o prihodima, porezima i doprinosima.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji/dosijeu imaju isključivo radnici koji su za to ovlašteni u Službi za pravne poslove i upravljanje ljudskim resursima/Službi za računovodstvo i finansije/Referent za upravljanje

	ljudskim resurima/Referent za obračun plata/Referent za finansijske poslove. Svako ovlaštenje utvrđuje se prema radnom mjesu i zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke/dosije imaju Rukovodioci službi, referenti službi i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u Službi za pravne poslove i upravljanje ljudskim resursima te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku (dosije) čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom; elektronske evidencije se čuvaju u sistemima s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s Listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za pravne poslove i upravljanje ljudskim resursima i Službe za računovodstvo i finansije	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika (osobe koje za Preduzeće obavljaju rad, a nisu u radnom odnosu), službe su dužne preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (službe moraju sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka**

	službe bez odlaganja, a najkasnije u roku od dva sata, obavještavaju Službenika za zaštitu ličnih podataka, putem e-pošte ili internog sistema - dostavljaju sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima **Procjena rizika** rukovodioci službi/Rukovodilac Službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac Službe za računovodstvo i finansije, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile službe). **Obavještavanje oštećenih radnika** (Ako povreda može uzrokovati štetu radnicima Služba za pravne poslove i upravljanje ljudskim resursima ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

c) Evidencija o obračunu i isplatama plaća i naknada plaća radnicima Preduzeća

Evidencije o ličnim podacima	Evidencija o obračunu i isplatama plaća i naknada plaća radnicima Preduzeća vodi se u SEEP-u/ Službi za računovodstvo i finansije.
Svrha obrade	Obrada se vrši isključivo u svrhu ostvarivanja prava iz radnog odnosa
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: ime i prezime, ime oca, adresa prebivališta, JMBG, opština stanovanja, koeficijent složenosti, godine staža i stopa minulog rada, radno mjesto i organizaciona jedinica, transakcijski račun zaposlenika, podaci o prihodima, doprinosima i porezu zaposlenika, faktor ličnog odbitka, iznos neto plate, iznos naknada, iznos obustava zaposlenika prema bankama, izvještaj o privremenoj spriječenosti za rad, šifra zaposlenika.

Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji/dosijeu imaju isključivo radnici koji su za to ovlašteni u Službi za računovodstvo i finansije/(Referent za obračun plata). Svako ovlaštenje utvrđuje se prema radnom mjesu i zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe za računovodstvo i finansije, Referent za obračun plaća i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u Službi za računovodstvi i finansije te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom; elektronske evidencije se čuvaju u sistemima s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s Listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za računovodstvo i finansije/Odjel za obračun plata	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika (osobe koje za Preduzeće obavljaju rad, a nisu u radnom odnosu), služba je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu ličnih podataka** (služba bez odlaganja obavještava, a najkasnije u roku

	od dva sata, Službenika za zaštitu ličnih podataka - dostavljaju sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** rukovodioci službi/Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za računovodstvo i finansije, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila služba). **Obavještavanje oštećenih radnika** (Ako povreda može uzrokovati štetu radnicima služba u kojoj se vrši obrada ih obavještava jasno, razumljivo i bez odlaganja: daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

d) Evidencija o obračunu i isplatama naknada članovima organa Preduzeća, komisijama i osobama angažovanim po drugim osnovama

Evidencije o ličnim podacima	Evidencija o obračunu i isplatama naknada članovima organa Preduzeća, komisijama i osobama angažovanim po drugim osnovama vodi se u SEPP-u/ Službi za računovodstvo i finansije u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu ostvarivanja prava izvan radnog odnosa
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: ime i prezime, JMBG, broj lične karte, organ koji je izdao i mjesto izdavanja, adresa stanovanja, opština stanovanja, transakcijski račun i banka kod koje se vodi isti, podaci o prihodima, porezima i doprinosima.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji/dosijeu imaju isključivo radnici koji su za to ovlašteni u Službi za računovodstvo i finansije/Referent za obračun plata/Referent za finansijske poslove.

	Svako ovlaštenje utvrđuje se prema radnom mjestu zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke ima, Referent za obračun plata, Rukovodilac službe za računovodstvo i finansije i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u službi te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom; elektronske evidencije se čuvaju u sistemima s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s Listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za računovodstvo i finansije/Odjel za obračun plata/Odjel za finansijske poslove	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika (članovi organa Preduzeća, komisije i osobe angažovane po drugim osnovama), služba je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu ličnih podataka** (služba bez odlaganja, najkasnije u roku od dva sata, obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako

	bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za računovodstvo i finansije, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila služba). **Obavještavanje članova organa Preduzeća, komisija i osoba angažovanih po drugim osnovama** (Ako povreda može uzrokovati štetu nadležna služba ih obavještava, razumljivo i bez odlaganja: daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka: preventivne mjere).

e) Evidencije o utuženim dužnicima koji se odnose na fizička lica iz tarifne kategorije Domaćinstva i fizička lica koja obavljaju samostalne djelatnosti

Evidencije o ličnim podacima	Evidencija o utuženim dužnicima koji se odnose na fizička lica iz tarifne kategorije „Domaćinstva" i fizička lica koja obavljaju samostalne djelatnosti vodi se u SEEP-u/ Službi za pravne poslove i upravljanje ljudskim resurima/Službi naplate i obračuna utroška vode/Službi za računovodstvo i finansijo, Odjeljenju IT u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu vođenja parničnog i izvršnog postupka pred nadležnim sudom, a u svrhu naplate potraživanja putem suda.
Način obrade	Obrada ličnih podataka može biti pisana (formiran spis) ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službama.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: ime i prezime, ime oca, adresa mjernog mjesta, transakcijski račun i banka kod koje se vodi, JMBG, broj lične karte, mjesto izdavanja, iznos tuženog duga i period na koji se dug odnosi, trenutni status sudskog predmeta, ID i PDV (ako ga po zakonu imaju), vrsta samostalne djelatnosti koju dužnik obavlja, datum tužbe, adresa mjernog mjesta, podaci o eventualnim uplatama duga i sporednih potraživanja. U zavisnosti od potreba postupka, a na

	zahtjev suda može se zatražiti dodatni identifikacioni podatak. Pored suda pred kojim se vodi postupak, lične podatke mogu tražiti i nadležni organi uprave (MUP, Porezna uprava FBiH, FIA) s ciljem identifikacije i prethodne provjere imovine lica.
Ovlaštenja za obradu i pristup	(Rukovodioci službi/Šef odjeljenja naplate, Glavni referent za pravne poslove i upravljanje ljudskim resursima, Referent za izvršni postupak, Referent za zastupanje i pravna pitanja, Administrator, Referent za naplatu I, Kontrolor blagajne, Glavni blagajnik, Blagajnik, Referent za naplatu III, Referent za reklamacije i informacije, Administrator operater II, Referent za kontakte sa korisnicima, Administrativni radnik u centru za potrošače, Referent za IT, IT aministrator Svako ovlaštenje utvrđuje se prema radnom mjestu i zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke imaju, Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe naplate i obračuna utroška vode, Rukovodilac službe za računovodstvo i finansije i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama (utuženi kupci) na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u službi koja je omogućila uvid te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencija u papirnom obliku (Ugovori, razni zahtjevi, zapisnici) čuvaju se zaključanim ormarima ili prostorijama s kontrolisanim pristupom, elektronske evidencije se čuvaju u sistemu s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za pravne poslove i upravljanje ljudskim resursima/Službe naplate i obračuna utroška vode/Službe računovodstva i finansija/Odjeljenja IT	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka utuženih dužnika nadležne službe, svaka iz svog domena, je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju,

	objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (nadležna služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu podataka** (nadležna služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe naplate i obračuna utroška vode, Rukovodilac službe za računovodstvo i finansije, Šef odjeljenja IT, i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode utuženog kupaca, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila nadležna Služba). **Obavještavanje utuženim dužnicima** (Ako povreda može uzrokovati štetu nadležna služba ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (Otklanjanje uzroka incidenta, uključujući izmjene procedura, unapređenje kontrole pristupnih prava, uklanjanje neovlašteno distribuiranih podataka, kao i provođenje preventivnih mjera radi sprečavanja ponavljanja incidenta).

f) Evidencija o kupcima/korisnicima usluga

Evidencije o ličnim podacima	Evidencija o kupcima/korisnicima vodi se u SEPP-u/Službi za pravne poslove i upravljanje ljudskim resursima/Službi za računovodstvo i finansije/Službi naplate, obračuna utroška vode i Odjeljenju IT u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu regulisanja obligaciono – pravnog odnosa između Preduzeća kao prodavca i korisnika/kupca.

Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službama.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: ime i prezime, ime oca, adresu stanovanja, adresa mjernog mjesta, broj vodomjera, broj i datum zaključenog ugovora, ID i PDV (ako ga po zakonu imaju), te ostale podatke po mogućnosti kao što su: broj lične karte, organ koji je izdao i mjesto izdavanja i trajanje. Ugovori sa korisnicima/kupcima čuvaju se u Službi naplate i obračuna utroška vode.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni odnosno kojima je u opisu radnog mjesta u Službi za pravne poslove i upravljanje ljudskim resursima, Službi za računovodstvo i finansije, Odjeljenju IT i u Službi naplate i obračuna utroška vode (Rukovodioci službi/Šef odjeljenja naplate, Referent za naplatu I, Kontrolor blagajne, Glavni blagajnik, Blagajnik, Referent za naplatu III, Referent za reklamacije i informacije, Administrator operater II, Referent za kontakte sa korisnicima, Administrativni radnik u centru za potrošače, Referent IT i administrativni radnik IT). Svako ovlaštenje utvrđuje se prema radnom mjestu zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke imaju Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za računovodstvo i finansije, Rukovodilac službe naplate i obračuna utroška vode, Šef Odjeljenja IT i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama (kupcima) na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u službi koja je omogućila uvid te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku (Ugovori, razni zahtjevi, zapisnici) čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom; elektronske

	evidencije se čuvaju u sistemima s korisničkim autentifikacijama i lozinkama. Čuvaju se u skladu s Listom kategorija registraturne građe s rokovima čuvanja.
Postupanje Službe za pravne poslove i upravljanje ljudskim resursima/Službe naplate i obračuna utroška vode/Službe za računovodstvo i finansije/Odjeljenja IT	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika/korisnika usluga, nadležna služba je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (nadležna Služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu podataka** (nadležna Služba bez odlaganja, a najkasnije u roku od dva sata obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** nadležne službe/Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Šef odjeljenje IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode kupaca, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtjeva prijavu, Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila nadležna služba). **Obavještavanje kupca/korisnika** (Ako povreda može uzrokovati štetu, nadležna služba ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). Ukoliko je šteta prouzrokovana kod većeg broja kupaca/korisnika, Uprava može razmotriti mogućnost da ih o tome obavijesti putem objave na službenoj web stranici ili slanjem e-mail obavijesti korisnicima. **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka;

	preventivne mjere).

g) Evidencija o obradi podataka snimljenih putem sistema video nadzora

Evidencije o ličnim podacima	Evidencija o obradi podataka snimljenih putem sistema video nadzora vrši se u SEEP-u.Videonadzor se vrši na ulazima i izlazima objekata Preduzeća, zajedničkim prostorijama, hodnicima i/ili vanjskim površinama u neposrednoj blizini objekta, isključivo radi zaštite osoba i imovine. Evidencija sadrži sliku, pokret, vrijeme i datum video zapisa. Videonadzor je u nadležnosti Službe za opšte poslove, unutrašnje zaštite i zaštite na radu.
Svrha obrade	Obrada se vrši isključivo u svrhu zaštite ljudi i imovine i ispunjenja zakonskih i podzakonskih odredbi iz oblasti zaštite ljudi i movine.
Način obrade	Podaci snimljeni putem videonadzora pohranjuju se na snimaču i isti se koriste i obrađuju u skladu sa Zakonom o zaštiti ličnih podataka kao i propisima koji regulišu ovu oblast, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: slika, pokret, vrijeme i datum video zapisa.
Ovlaštenja za obradu i pristup	Pristup snimcima je ograničen i dozvoljen samo ovlaštenim radnicima Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/ Šef odjeljenja za opšte poslove i unutrašnju zaštitu.
Uvid u lične podatke	Uvid u lične podatke imaju Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Šef odjeljenja za opšte poslove i unutrašnju zaštitu i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, samo u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu ili sistemskom logu (datum, vrsta snimka, vrijeme nastanka, vrijeme uvida, svrhu i obim obrade, u skladu sa Odlukom). Evidencija se vodi na mjesečnom nivou i čuva se u službi koja je omogućila uvid te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH mora biti dostupna.
Čuvanje dokumentacije	Snimljeni materijal se automatski pohranjuje u Službi za

	opšte poslove, unutrašnju zaštitu i zaštitu na radu. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja (minimalno 30 dana)
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka prikupljenih putem videonadzora nadležna služba je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak snimka, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.: identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (nadležna služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke/snimke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu ličnih podataka** (nadležna služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštite na radu/Šef odjeljenja za opšte poslove i unutrašnju zaštitu, Šef odjeljenje IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode osoba sa snimka, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila nadležna služba). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

h) Evidencija o obradi ličnih podataka snimljenih putem sistema audio zapisa telefonskog razgovora

Evidencije o ličnim podacima	Evidencije o obradi ličnih podataka snimljenih putem audio zapisa telefonskog razgovora vrši se u Sektoru za

	investicije i tehničke poslove/ Službi za elektro održavanje/ Odjeljenju IT. Lični podaci obrađuju se na osnovu direktnih poziva/snimanja poziva (ime i prezime korisnika, adresa mjernog mjesta, šifra korisnika, kontakt telefon, te drugi podaci iz sadržaja razgovora a koje korisnik izgovori: (žalbe, zahtjevi, pitanja, izjave).
Svrha obrade	Obrada se vrši isključivo u svrhu evidentiranja, prijema i obrade hitnih dojava te unapređenja usluga.
Način obrade	Podaci snimljeni putem audio zapisa pohranjuju se na snimaču i isti se koriste i obrađuju u skladu sa Zakonom o zaštiti ličnih podataka kao i propisima koji regulišu ovu oblast, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeće vrste ličnih podataka: ime i prezime korisnika, adresa mjernog mjesta, šifra korisnika, kontakt telefon.
Ovlaštenja za obradu i pristup	Pristup snimcima je ograničen i dozvoljen samo ovlaštenim radnicima u Službi za elektro održavanje/IT administrator.
Uvid u lične podatke	Uvid u lične podatke imaju Rukovodilac službe za elektro održavanje, IT administrator i Izvršni direktor za investicije i tehničke poslove. Mogu biti dostavljeni na zahtjev Suda ili drugih nadležnih organa.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (datum, vrsta snimka, vrijeme nastanka, vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na mjesečnom nivou i čuva se u službi koja je omogućila uvid te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja (minimalno 30 dana)
Postupanje Službe za elektro održavanje/ Odjeljenje IT/IT administrator	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka prikupljenih putem audio zapisa telefonskog razgovora nadležna služba je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak snimka, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata).

	Dokumentovanje incidenta (nadležna služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke/snimke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu podataka** (nadležna služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** (Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima/Rukovodilac službe za elektro održavanje, Šef odjeljenja IT, IT administrator i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode osoba sa snimka, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu, Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju je sačinila nadležna služba). **Preduzimanje korektivnih mjera** (Identifikacija i uklanjanje uzroka incidenta kroz izmjenu postojećih procedura, ograničavanje i redefinisanje pristupnih prava, brisanje pogrešno distribuiranih podataka, uz uvođenje odgovarajućih preventivnih mjera)

i) Evidencije o obradi ličnih podataka lica koja posjećuju službene prostorije KJKP „Vodovod i kanalizacija“ d.o.o. Sarajevo

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka lica koja posjećuju službene prostorije Preduzeća vrši se u SEPP-u evidentiranjem podataka prilikom ulaska u službene prostorije lica koji nisu radnici Preduzeća. Vodi se u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Odjeljenje za opšte poslove i unutrašnju zaštitu u skladu sa propisanim ovlaštenjima.
Svrha obrade	Obrada se vrši isključivo u svrhu obezbjeđenja sigurnosti osoba, imovine i informacija unutar službenih prostorija Preduzeća.
Način obrade	Obrada ličnih podataka može biti ručna uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	U evidenciji se obrađuju samo podaci nužni za ostvarivanje svrhe obrade, i to: ime i prezime, broj lične karte, datum, vrijeme dolaska i odlaska, ime i prezime osobe koju posjećuje te razlog posjete

	(privatno/službeno).
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo radnici koji su za to ovlašteni u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu (Šef odjeljenje za opšte poslove i unutrašnju zaštitu/Dežurni radnik/Zaštitar).
Uvid u lične podatke	Uvid u lične podatke/dosije zaposlenih ima, Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Šef odjeljenja za opšte poslove i unutrašnju zaštitu i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi na mjesečnom nivou i čuva se u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka lica koja posjećuju službene prostorije Služba za opšte poslove, unutrašnju zaštitu i zaštitu na radu je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (Bez odlaganja utvrditi da li je došlo do povrede zaštite podataka, uključujući neovlašteni pristup, neovlašteno otkrivanje ili gubitak uređaja, te identifikovati kategorije kompromitovanih podataka i njihov obim.). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; (zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose). **Obavještavanje Službenika za zaštitu podataka** (služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao

	i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima/ Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Šef odjeljenja za opšte poslove i unutrašnju zaštitu/Šef odjeljenje IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ukoliko se utvrdi da povreda podliježe obavezi prijavljivanja, Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja pripadajuću dokumentaciju sačinjenu od strane nadležnih službi). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu nosiocu podataka nadležna služba ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena internih procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

j) Evidencija o obradi ličnih podataka radnika KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo koji obavljaju poslove fizičke i tehničke zaštite, periodičnoj provjeri korištenja vatrenog oružja, psiho-fizičkoj sposobnosti i stručnoj obuci istih

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka radnika KJKP „Vodovod i kanalizacija" d.o.o. Sarajevo koji obavljaju poslove fizičke i tehničke zaštite, periodičnoj provjeri korištenja vatrenog oružja, psiho-fizičkoj sposobnosti i stručnoj obuci istih vrši se evidentiranjem podataka u pisanom obliku (knjiga). Vodi se u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/ Šef odjeljenja za opšte poslove i unutrašnju zaštitu
Svrha obrade	Obrada se vrši isključivo u svrhu obezbjeđenja sigurnosti ljudi, imovine i poslovnih procesa, kao i radi ispunjavanja posebnih uslova koje radnici moraju ispunjavati za obavljanje poslova fizičke i tehničke zaštite, a sve u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se	U evidenciji se obrađuju samo podaci nužni za

obrađuju	ostvarivanje svrhe obrade, i to: ime i prezime, ime i prezime komisije koja vrši propisane provjere ili naziv institucije, rezultate provjera, datum vršenja provjera.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo radnici koji su za to ovlašteni u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/ Šef odjeljenja za opšte poslove i unutrašnju zaštitu
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe/ Šef odjeljenja i Izvršni direktor za ekonomske pravne poslove. Uvid u lične podatke može biti omogućen: radnicima na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi na mjesečnom nivou i čuva se u Službi za opšte poslove, unutrašnju zaštitu i zaštite na radu, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštite na radu u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika Službe za opšte poslove, unutrašnju zaštitu i zaštite na radu/ Odjeljenje za opšte poslove i unutrašnju zaštitu je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. Neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka – dostavlja sve dostupne informacije kao

	i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštite na radu, Šef odjeljenja za opšte poslove i unutrašnju zaštitu, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile službe). **Obavještavanje oštećenih radnika** (Ako povreda može uzrokovati štetu nosiocu podataka nadležna služba ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

k) Evidencije o ljekarskim pregledima zaposlenika raspoređenih na radna mjesta sa posebnim uslovima rada

Evidencije o ličnim podacima	Evidencije o obradi ličnih podataka o ljekarskim pregledima zaposlenika raspoređenih na radna mjesta sa posebnim uslovima rada, vrše se prilikom obavljanja obaveznih sistematskih i periodičnih ljekarskih pregleda zaposlenika, koje vrši ovlaštena zdravstvena ustanova. Podaci se dostavljaju poslodavcu u obliku izvještaja o zdravstvenoj sposobnosti za rad, bez navođenja dijagnoze, u skladu sa Zakonom. Vodi se u SEPP-u/Službi za opšte poslove, unutrašnju zaštitu i zaštite na radu
Svrha obrade	Obrada se vrši isključivo u svrhu evidentiranja i praćenja zdravstvene sposobnosti zaposlenika, posebno onih raspoređenih na radna mjesta sa posebnim uslovima rada, te u cilju ispunjavanja zakonskih obaveza Preduzeća u vezi sa zaštitom zdravlja i sigurnosti na radu, a sve u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.

Obim ličnih podataka koji se obrađuju	U evidenciji se obrađuju samo podaci nužni za ostvarivanje svrhe obrade, i to: ime i prezime, naziv institucije, rezultate provjera, datume vršenja provjera.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo radnici koji su za to ovlašteni u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/ Šef odjeljenje za zaštitu na radu/Referent za zaštitu na radu.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu, Šef odjeljenja za zaštitu na radu, Referent za zaštitu na radu i Izvršni direktor za ekonomske i pravne poslove. Uvid u lične podatke može biti omogućen: radnicima na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi na godišnjem nivou i čuva se u Službi za opšte poslove, unutrašnju zaštitu i zaštite na radu, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštite na radu u slučaju povrede ličnih podataka	S obzirom na to da je riječ o obradi posebnih kategorija ličnih podataka, u slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika Služba za opšte poslove, unutrašnju zaštitu i zaštite na radu je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. Neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka – dostavlja sve dostupne informacije kao

	i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima/Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštite na radu, Šef odjeljenja za zaštitu na radu, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile Službe). **Obavještavanje oštećenih radnika** (Ako povreda može uzrokovati štetu nosiocu podataka, Rukovodilac Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu, ih obavještava jasno, razumljivo i bez odlaganja: daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** uklanjanje uzroka incidenta npr. Izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

l) Evidencija o kandidatima prijavljenim na Javni oglas za prijem u radni odnos kao i za imenovanja u organe Preduzeća (Uprava, Nadzorni odbor, Skupština, Odbor za reviziju)

Evidencije o ličnim podacima	Evidencije o obradi ličnih podataka o kandidatima prijavljenim na Javni oglas za prijem u radni odnos kao i za imenovanja u organe Preduzeća (Uprava, Nadzorni odbor, Skupština, Odbor za reviziju) vode se u pisanom obliku na osnovu prijavne dokumentacije dostavljene na javni oglas. Za obradu evidencija zadužen je sekretar komisije koju imenuje direktor za potrebe provodenja javnog oglasa.
Svrha obrade	Prikupljaju se u svrhu regulisanja radno-pravnog statusa i ostvarenja prava i obaveza iz radnog odnosa, a sve u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite.
Obim ličnih podataka koji se obrađuju	U evidenciji se obrađuju samo podaci nužni za ostvarivanje svrhe obrade, i to: ime i prezime (djevojačko prezime) i ime oca, mjesto, dan, mjesec i

	godina rođenja, adresa stanovanja /prebivalište ili boravište/, državljanstvo, vrsta završene škole i stepen stručne spreme, naziv radnog mjesta, broj telefona i email adresa, datum zasnivanja i prestanka radnog odnosa, učešće u oružanim snagama tokom rata 1992. – 1995.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo sekretar i članovi/zamjenici imenovanih komisija iz reda radnika Preduzeća.
Uvid u lične podatke	Uvid u lične podatke imaju članovi komisija/ zamjenski članovi i sekretar komisije. Uvid u lične podatke može biti omogućen kandidatima koji se prijavljuju na javni oglas, u skladu sa poslovnikom o radu komisije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi u toku trajanja javnog oglasa i čuva se kod sekretara komisije, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije u papirnom obliku čuvaju se u zaključanim ormarima ili prostorijama s kontrolisanim pristupom kod sekretara, a nakon završetka konkursne procedure dostavljaju se Službi za pravne poslove i upravljanje ljudskim resursima. Predmetna dokumentacija se čuva u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje Komisije u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika komisija je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. Neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Komisija mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Komisija bez odlaganja obavještava Službenika za zaštitu ličnih podataka – dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima.

	Procjena rizika Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima/predsjednik komisije/ i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile Službe). **Obavještavanje oštećenih kandidata** (Ako povreda može uzrokovati štetu nosiocu podataka komisija daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. Izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

m) Evidencija o intervencijama kod korisnika usluga

Evidencije o ličnim podacima	Evidencije o intervencijama kod korisnika usluga se vodi u svim pogonima/sektorima kroz elektronsku bazu podataka gdje se pohranjuju podaci o intervencijama kod korisnika usluga radi osiguranja kvalitete usluga, otklanjanja kvarova i sigurnosti korisnika.
Svrha obrade	Obrada se vrši isključivo u svrhu analize, praćenja i realizacije intervencija, odgovornosti i unapređenja usluga, a sve u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u nadležnoj službi.
Obim ličnih podataka koji se obrađuju	Na zapisima koji se popunjavaju na terenu evidentiraju se podaci o kupcu (ime i prezime kupca, kontakt telefon, adresa mjernog mjesta kupca), vrsta aktivnosti na mjernom mjestu/unutrašnjoj instalaciji. Za pripremu radnog naloga koriste se podaci iz baze Preduzeća koje prikupljaju drugi sektori i službe.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo rukovodioci službi i radnici koji su za to ovlašteni. Na zahtjev službi, a u skladu sa internim procedurama, od kupca (vlasnika nekretnine) se pribavljaju podaci o broju lične karte i mjestou izdavanja, radi regulisanja ugovornih odnosa.

Uvid u lične podatke	Uvid u lične podatke imaju rukovodioci nadležnih službi/ šefovi službi i izvršni direktori. Uvid u lične podatke može biti omogućen: korisnicima usluga na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi na mjesečnom nivou i čuva se u nadležnim službama, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Evidencije/zapisnici u papirnom obliku čuvaju se u prostorijama s kontrolisanim pristupom. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje nadležnih službi u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika nadležne službe su dužne preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. Neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (nadležna Služba mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (nadležna služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka – dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursim, Rukovodioci nadležne službe/ Šef nadležne službe, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da

	povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile službe). **Obavještavanje nosilaca podataka** (Ako povreda može uzrokovati štetu nosiocu podataka nadležne službe jasno, razumljivo i bez odlaganja: daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. Izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

n) Evidencija o obradi ličnih podataka prikupljenih putem web stranice Preduzeća

Evidencije o ličnim podacima	Evidencije o obradi ličnih podataka prikupljenih putem web stranice Preduzeća vrši se u Sektoru za investicije i tehničke poslove. U Odjeljenju IT, prikupljanje se odvija na strukturisan i tehnički precizan način, prilikom direktne interakcije sa korisnicima putem web stranice Preduzeća i servisa Provjera računa.
Svrha obrade	U svrhu pružanja i unapređenja usluga, održavanja sigurnosti i funkcionalnosti web stranice, dobivanja statističkih podataka vezanih za korištenje web stranice te pružanja usluge provjere računa.
Način obrade	Prilikom direktne interakcije sa korisnicima putem web stranice Preduzeća i servisa
Obim ličnih podataka koji se obrađuju	Prikupljaju se sljedeći podaci: ime i prezime, šifra kupca, kućna ili poslovna adresa. Automatski se prikupljaju podaci o računaru: IP adresa posjetioca, tip preglednika, ime domene, vrijeme pristupa i adrese web stranica.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo radnici koji su za to ovlašteni u Odjeljenju IT/IT administratori.
Uvid u lične podatke	Uvid u lične podatke ima Šef odjeljenja, IT administrator, Izvršni direktor za investicije i tehničke poslove i direktor Preduzeća. Uvid u lične podatke može biti omogućen: korisnicima usluga na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu.

	Evidencija se vodi na mjesečnom nivou i čuva se u Odjeljenju IT, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Onoliko koliko je neophodno za ostvarivanje svrhe prikupljanja. Po isteku roka podaci se brišu ili anonimiziraju, osim ako je daljna obrada zakonska obaveza.
Postupanje nadležnih službi u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede prikupljenih ličnih podataka Odjeljenje IT je dužna preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje). **Dokumentovanje incidenta** (nadležna Služba u Sektoru mora sastaviti zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (nadležna Služba bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode lica koja posjećuju službene prostorije, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile Službe sa definisanim poduzetim koracima). **Obavještavanje nosilaca podataka** (Ako povreda može uzrokovati štetu nosiocu podataka nadležna Služba ih obavještava jasno, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

o) Evidencije o obradi ličnih podataka za potrebe komunikacije s medijima i javnošću

Evidencije o ličnim podacima	Evidencije o obradi ličnih podataka za potrebe komunikacije s medijima i javnošću prikupljaju se u Odjelu za odnose sa javnošću, putem telefona, službenog e-maila, djelimično automatski s pripadajućom ručnom datotekom, (ime i prezime, naziv medijske kuće/organizacije, funkcija, e-mail adresa, broj telefona, fotografije i video zapisi sa događaja).
Svrha obrade	U svrhu distribucije saopštenja za javnost, slanja poziva na konferencije za medije i druge javne događaje, odgovaranja na novinarske upite i zahtjeve za informacije u skladu sa Zakonom o zaštiti ličnih podataka BiH.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u Sekretarijatu.
Obim ličnih podataka koji se obrađuju	Pri realizaciji aktivnosti komunikacije sa medijima i javnošću, Preduzeće može obrađivati sljedeće kategorije ličnih podataka: identifikacioni podaci zaposlenih ili ovlaštenih predstavnika Preduzeća (službeni kontak telefon, email adresa, naziv radnog mjesta), podaci neophodni za davanje službenih izjava i komunikaciju s medijima (potpisane izjave, fotografije ovlaštenih predstavnika Preduzeća-ukoliko je potrebno za medijske nastupe, video i audio snimci sa javnih istupa, konferencija ili saopštenja), podaci novinara i predstavnika medija za potrebe komunikacije (kontakt podaci koje novinar dobrovoljno dostavi radi komunikacije), podaci objavljeni u svrhu informisanja javnosti (lični podaci koji se, uz saglasnost ili pravni osnov, objavljuju u saopštenjima, javnim obavještenjima ili na službenim kanalima Preduzeća).
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup evidenciji imaju isključivo Odjel za odnose sa javnošću/Glavni PR Preduzeća/ PR Preduzeća. Svako ovlaštenje utvrđuje se individualno, prema funkciji i radnim zadacima zaposlenog.
Uvid u lične podatke	Uvid u lične podatke ima Referent za pravne i administrativne poslove organa uprave i direktor Preduzeća. Uvid u lične podatke može biti omogućen: osobama na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti, isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane

	svrhe.
Evidencije	Svi uvidi se evidentiraju u odgovarajućem zapisu. Evidencija se vodi na godišnjem nivou.
Čuvanje dokumentacije	Evidencije i snimci se čuvaju u prostorijama s kontrolisanim pristupom/računaru koji je osiguran lozinkom. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje/Odjela za odnose s javnošću u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede prikupljenih ličnih podataka u Odjelu za odnose sa javnošću se poduzimaju sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; zaključavanje, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (u Odjelu za odnose sa javnošću sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Odjel za odnose sa javnošću bez odlaganja obavještava Službenika za zaštitu ličnih podataka - dostavlja sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Glavni PR Preduzeća, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode nosilaca ličnih podataka, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja dokumentaciju koju su sačinile Službe). **Obavještavanje nosilaca podataka** (Ako povreda može uzrokovati štetu nosiocu podataka Glavni PR Preduzeća, razumljivo i bez odlaganja; daje informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

p) Evidencije o obradi ličnih podataka za potrebe online podrške i komunikacije sa eksternim subjektima

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka za potrebe online podrške i komunikacije sa eksternim subjektima, a koji su zapremljeni od trećih lica vode se na nivou Preduzeća na zvaničnim e-mail adresama Preduzeća (info@viksa.ba,press@viksa.ba, komunikacije@viksa.ba)
Svrha obrade	Rukovodioci službi obavljaju koordinaciju između eksternih subjekata i nadležnih službi Preduzeća, kao krajnjih korisnika podataka i informacija dostavljenih putem zvaničnih e-mail adresa Preduzeća. Rukovodioci i zaduženi radnici eksternim subjektima elektronske upite, dostavljene putem zvaničnih e-mail adresa Preduzeća, koriste za interne statističke svrhe, unapređenja usluga i poslovanja.
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u službi.
Obim ličnih podataka koji se obrađuju	Zaprima se sljedeća elektronska pošta: sve vrste zahtjeva kao što su (uključenja kupca, odjave mjernog mjesta, promjene imena nosioca računa usluge, usluga e-račun, izlazak tehničkih službi na teren/ hitne intervencije/ obilježavanje podzemnih instalacija, verifikacije mjerila, povrat novca, konfirmacije i sl.), sve vrste molbi kao što su (odgode plaćanja, reprogram duga, provjere statusa korisnika, provjere knjiženja uplata, stanje na korisničkom računu, analitičke kartice, duplikati računa za uslugu, prijem u radni odnos i sl.), reklamacije kupaca po svim osnovama (očitanje potrošnje, obračun potrošnje, stanje na korisničkom računu, ostale usluge koje pruža Preduzeće), dokaze o uplati (potrošnja, usluge i sl.). Navedena elektronska pošta sadrži e-mail adresu pošiljaoca, ime prezime pošiljaoca, te može sadržavati u okviru e-maila ili u okviru pratećeg priloga: šifru kupca, adresu, kontakt telefon, broj transakcijskog računa, broj lične karte, broj mjernog mjesta.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo ovlašteni zaposlenici, rukovodioci i direktori, u okviru svojih radnih zadataka i dodjeljenih ovlaštenja, uz primjenu propisanih mjera zaštite podataka.
Uvid u lične podatke	Uvid u lične podatke imaju Rukovodioci službi, direktori Preduzeća i zaposlenici koji su time zaduženi. Uvid u lične podatke može biti omogućen: eksternim subjektima na koje se podaci odnose, u skladu s njihovim pravima iz Zakona, nadležnim organima vlasti,

	isključivo na temelju pisanog zahtjeva i zakonskog ovlaštenja, trećim licima, samo ako postoji jasan pravni osnov ili pisana saglasnost nosioca podataka, osim ako zakon ne propisuje drugačije.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na godišnjem nivou i čuva se u nadležnim službama te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Elektronski upit (bez priloga) eksternog subjekta se arhivira, u elektronskoj formi. Dozvolu za unos podataka u internu bazu podataka (MONV, KANA i WEB Aplikacije) imaju uposlenici koji su za to ovlašteni. Uposlenici iz nadležnih službi Preduzeća, koji imaju pristup za sve podatke o kupcima, imaju mogućnost čitanja podataka dostupnih i u bazi. Čuva se u skladu s Listom kategorija registraturne građe s rokovima čuvanja
Postupanje službi za podršku eksternim subjektima u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika, nadležne službe su dužne preduzeti sljedeće mjere: **U saradnji Šefom odjeljenja IT izvršiti hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodioci nadležnih službi, Šef odjeljenja IT i Službenik za zaštitu ličnih

	podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih eksternih korisnika** (Ako povreda može uzrokovati štetu eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

q) Evidencije o obradi ličnih podataka u Odjelu za internu reviziju

Evidencije o ličnim podacima	Najčešći način prikupljanja je putem pristupa postojećim poslovnim i upravljačkim dokumentima, koji sadrže lične podatke.
Svrha obrade	U skladu sa Planom rada Odjela za internu reviziju, u svrhu provođenja internih revizija vrši se obrada podataka uvidom u iste, u cilju izvještavanja Odbora za reviziju.
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u Odjelu.
Obim ličnih podataka koji se obrađuju	Kadrovska dokumentacija (ugovori o radu, evidencije prisustva, rješenja, odluke i druga relevantna dokumentacija), finansijska dokumentacija (izvještaji, interni izvještaji koji uključuju identitet zaposlenih, podaci o ugovornim partnerima, podaci o isplatama zaposlenicima i druga relevantna dokumentacija).
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Odjelu za inernu reviziju (Šef odjela interne revizije i interni revizor).
Uvid u lične podatke	Odjel za internu reviziju ima potpun i cjelovit uvid u svu evidenciju javnog preduzeća potrebnu za obavljanje poslova, isključivo, u skladu sa zakonskim ovlaštenjima i internim procedurama (Zakon o javnim preduzećima FBiH)
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Odjel za internu reviziju ne izdaje lične podatke na uvid.

Čuvanje dokumentacije	U skladu sa Listom kategorija registraturne građe sa rokovima čuvanja.
Postupanje Odjela za za internu reviziju u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka radnika, Odjel za internu reviziju je dužan preduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Šef odjela interne revizije, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

r) Evidencija o obradi ličnih podataka na Protokolu Preduzeća

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka na Protokolu Preduzeća vrši se u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/ Odjeljenje za opšte poslove i unutrašnju zaštitu. Vođenje evidencije u pisanoj formi putem knjige protokola obuhvata sistematsko evidentiranje sve pristigle, obrađene, proslijeđene, otpremljene i arhivirane dokumentacije. U knjigu protokola unose se podaci o dokumentima koji mogu sadržavati informacije o zaposlenima, poslovnim partnerima, klijentima, korisnicima usluga, kandidatima za posao, kao i drugim fizičkim licima koja učestvuju u komunikaciji sa Preduzećem. Evidentirani podaci mogu uključivati: ime i prezime, adresu prebivališta, kontakt telefon, e-mail adresu, broj lične karte, matični broj, potpis, kao i druge informacije sadržane u priloženim dokumentima. Pored pisane evidencije, paralelno se vodi i elektronska evidencija, koja omogućava bržu pretragu, obradu i arhiviranje podataka, uz poštovanje važećih zakonskih propisa o zaštiti podataka o ličnosti. Obje evidencije (pisana i elektronska) vode se sa ciljem obezbjeđenja transparentnosti, sljedivosti i odgovornosti u postupanju sa dokumentacijom.
Svrha obrade	Pravilno evidentiranje prijema, obrade, distribucije i arhiviranja dokumentacije.
Način obrade	Obrada ličnih podataka može biti ručna ili elektronska, uz primjenu propisanih tehničkih i organizacijskih mjera zaštite.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Odjeljenje za opšte poslove i unutrašnju zaštitu/ Referent za administrativne poslove.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Šef Odjeljenja za opšte poslove i unutrašnju zaštitu i Izvršni direktor za ekonomske i pravne poslove. Evidencije mogu biti dostavljene po nalogu pravosudnih organa, kao i po zahtjevu ili molbi drugih učesnika u postupku.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na godišnjem nivou i čuva se u službi te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.

Čuvanje dokumentacije	U skladu sa Listom kategorija registraturne građe sa rokovima čuvanja.
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka zaprimljenih putem protokola, u Odjelu će se poduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za opšte poslove , unutrašnju zaštitu i zaštitu na radu, Šef odjeljenja za opšte poslove i unutrašnju zaštitu, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu radnicima i eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

s) Evidencija o obradi ličnih podataka u arhivi Preduzeća

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka u arhivi Pareduzeća vrši se u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Odjeljenje za opšte poslove i unutrašnju zaštitu. Vođenje evidencije u pisanoj formi putem Arhivske knjige obuhvata sistematsko evidentiranje sve pristigle dokumentacije koja je prethodno prošla kroz protokolarnu i obradu ostalih organizacionih jedinica Preduzeća, a može sadržavati lične podatke zaposlenih, bivših zaposlenih, kandidata za posao, poslovnih partnera, korisnika usluga, klijenata i drugih fizičkih lica koja su bila u kontaktu sa Preduzećem. Ovi dokumenti mogu sadržavati: ime i prezime, adresu, kontakt telefon, email, broj lične karte, matični broj, potpis, informacije o zaposlenju, ugovorima, projektima, pravima i obavezama, kao i druge lične podatke sadržane u službenim ili pratećim dokumentima. Dokumentacija se u arhivu prenosi iz drugih organizacionih jedinica Preduzeća, nakon što istekne njen period aktivne upotrebe.
Svrha obrade	Obrada ličnih podataka u arhivi vrši se u svrhu dugoročnog čuvanja, zaštite i upravljanja dokumentacijom u skladu sa zakonskim obavezama, internim aktima i rokovima definisanim u Listi kategorija registraturne građe. Cilj je očuvanje dokumentacionog kontinuiteta i omogućavanje pristupa arhivskoj građi u zakonom dozvoljenim slučajevima.
Način obrade	Obrada ličnih podataka je ručna uz primjenu propisanih tehničkih i organizacijskih mjera zaštite.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Službi za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Odjeljenje za opšte poslove i unutrašnju zaštitu/ arhivar.
Uvid u lične podatke	Uvid i lične podatke ima Rukovodilac službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu/Šef Odjeljenja za opšte poslove i unutrašnju zaštitu i Izvršni direktor za ekonomske i pravne poslove. Dokumentacija iz arhive može se izdavati isključivo po nalogu nadležnih pravosudnih i inspekcijskih organa, na osnovu zahtjeva ovlašćenih lica unutar Preduzeća, po pismenom zahtjevu fizičkih lica na koje se podaci odnose, ukoliko postoji zakonski osnov i identitet je potvrđen, po zahtjevu drugih lica u postupku, uz prethodnu pravnu provjeru osnova zahtjeva.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u

	odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na godišnjem nivou i čuva se u Odjelu te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	U skladu sa Listom kategorija registraturne građe sa rokovima čuvanja. Po isteku propisanih rokova čuvanja, dokumentacija se ili uništava uz zapisnik, ili se trajno arhivira ukoliko ima dugoročnu (trajnu) vrijednost.
Postupanje Službe za opšte poslove, unutrašnju zaštitu i zaštitu na radu u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka zaprimljenih putem protokola, u Odjelu će se poduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za opšte poslove , unutrašnju zaštitu i zaštitu na radu, Šef odjeljenja za opšte poslove i unutrašnju zaštitu, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu radnicima i eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu).

	Preduzimanje korektivnih mjera (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

t) Evidencija o obradi ličnih podataka za korisnike usluga priključenja na vodovodnu i kanalizacionu mrežu

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka za korisnike usluga priključenja na vodovodnu i kanalizacionu mrežu vrši se u Sektoru za investicije i tehničke poslove, Pogonu „Vodovod" i Pogonu „Kanlizacija" i SEPP-u kroz elektronsku bazu podataka gdje se pohranjuju podaci.
Svrha obrade	Obrada se vrši isključivo u svrhu analize, praćenja i realizacije intervencija, odgovornosti i unapređenja usluga da se osiguraju uslovi da budući korisnik ima uredno i kvalitetno snabdijevanje vodom i odvođenje otpadnih voda a sve u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u nadležnoj službi.
Obim ličnih podataka koji se obrađuje	Prikuplja se sljedeće vrste podataka za korisnike usluga priključenja; građevinska dozvola, potvrda ili odobrenje nadležnog općinskog organa da se objekat može priključiti na vodovodnu/kanalizacionu mrežu ako korisnik nema pravosnažnu građevinsku dozvolu, kopija katastarskog plana ili lokacija objekta, lokacija objekta ucrtana na katastar podzemnih instalacija, ovjerena situacija iz Glavnog projekta sa pečatom Tehničkog sekretara našeg Preduzeća, uzdužni profil iz Glavnog projekta, zahtjev za fizička lica (ime i prezime korisnika, kontakt telefon, adresu i vrstu aktivnosti priključenja)
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Službi za tehničke poslove, projektovanje i nadzor.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe za tehničke poslove projektovanje i nadzor i Izvršni direktor za investicije i tehničke poslove. Dokumentacija iz arhive može se izdavati isključivo po nalogu nadležnih pravosudnih i inspekcijskih organa, na osnovu zahtjeva ovlašćenih lica unutar Preduzeća, po pismenom zahtjevu fizičkih lica na koje se podaci odnose, ukoliko postoji zakonski osnov i identitet je potvrđen, po zahtjevu drugih lica u postupku, uz prethodnu pravnu provjeru osnova zahtjeva.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane

	neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi na godišnjem nivou i čuva se u službi, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	U skladu sa Listom kategorija registraturne građe sa rokovima čuvanja.
Postupanje Službe za tehničke poslove, projektovanje i nadzor u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka zaprimljenih putem protokola, u službi će se poduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za tehničke poslove, projektovanje i nadzor i Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu radnicima i eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu).

	Preduzimanje korektivnih mjera (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

u) Evidencija o obradi ličnih podataka za potrebe provođenja javnih nabavki

Evidencije o ličnim podacima	Evidencija o obradi ličnih podataka za potrebe provođenje javnih nabavki vrši se SEPP-u kroz elektronsku bazu podataka gdje se pohranjuju podaci.
Svrha obrade	Obrada se vrši isključivo u svrhu planiranja, provođenja i realizacije postupka javnih nabavki, uključujući pripremu tenderske dokumentacije, evaluaciju ponuda, donošenje odluka, zaključenje i praćenje realizacije ugovora, a sve u skladu sa zakonskim i podzakonskim propisima koji uređuju oblast javnih nabavki i zaštite ličnih podataka.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u nadležnoj službi.
Obim ličnih podataka koji se obrađuje	Obrađuju se samo podaci nužni za ostvarivanje svrhe obrade, i to najčešće: ime i prezime, naziv pravnog lica, kontakt podaci (telefon, e-mail), podaci iz ličnih dokumenata ako su potrebni (JMBG, ako je zakonski osnovano), podaci o stručnoj kvalifikaciji i referencama, podaci o finansijskoj sposobnosti, izjave i uvjerenja nadležnihorgana, te drugi podaci dostavljeni u okviru ponude ili zahtjeva za učešće.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Službi za javne nabavke. Svako ovlaštenje utvrđuje se u skladu sa radnim mjestom i dodjeljenjim zadacima.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe za nabavku i Izvršni direktor za ekonomske i pravne poslove. Dokumentacija iz arhive može se izdavati isključivo po nalogu nadležnih pravosudnih i inspekcijskih organa, na osnovu zahtjeva ovlašćenih lica unutar Preduzeća, po pismenom zahtjevu fizičkih lica na koje se podaci odnose, ukoliko postoji zakonski osnov i identitet je potvrđen, po zahtjevu drugih lica u postupku, uz prethodnu pravnu provjeru osnova zahtjeva.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim

	obrade). Evidencija se vodi na godišnjem nivou i čuva se u službi, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Dokumentacija u papirnom obliku čuva se u zaključanim ormarima ili prostorijama sa kontrolisanim pristupom, dok se elektronski podaci čuvaju u informacionim sistemima zaštićenim autentifikacijom i kontrolom pristupa Podaci se čuvaju u skladu sa važećim propisima i internim aktima i u skladu sa Listom kategorija registraturne građe sa rokovima čuvanja.
Postupanje Službe za nabavke u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka zaprimljenih putem protokola, u službi za nabavke će se poduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** (Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** (Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe za nabavku, Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu radnicima i eksternim korisnicima potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka

	incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

v) Evidencije o kontroli nelegalne potrošnje komunalnih/vodnih usluga (fizička lica iz kategorije „Domaćinstva" i fizička lica koja obavljaju samostalne djelatnosti, ostali korisnici i privredni subjekti)

Evidencije o ličnim podacima	Evidencija o obradi nelegalne potrošnje komunalnih/vodnih usluga (fizička lica iz kategorije „Domaćinstva" i fizička lica koja obavljaju samostalne djelatnosti, ostali korisnici i privredni subjekti vodi se SEPP-u/Služba naplate i obračuna utroška vode kroz elektronsku bazu podataka gdje se pohranjuju podaci.
Svrha obrade	Obrada se vrši isključivo u svrhu otkrivanja, dokazivanja i sprečavanja nelegalne potrošnje komunalnih/vodnih usluga, vođenja postupka kontrole, obračunaštete i pokretanja odgovarajućih postupaka, u skladu sa važećim zakonskim i podzakonskim propisima, kao i drugim općim aktima koji uređuju ovu oblast.
Način obrade	Obrada ličnih podataka može biti ručna i elektronska uz primjenu propisanih tehničkih i organizacijskih mjera zaštite u nadležnoj službi.
Obim ličnih podataka koji se obrađuje	Obrađuju se samo podaci nužni za ostvarivanje svrhe i to najčešće za fizička/pravna lica ime i prezime, adresa stanovanja, broj korisničkog računa i šifre potrošača, kontakt podaci, podaci o mjernom mjestu i potrošnji, zapisnici o kontroli, fotografije sa terena, podaci o utvrđenim nepravilnostima, podaci o obračunu štete, ID/PDV broj, vrsta djelatnosti.
Ovlaštenja za obradu i pristup	Ovlaštenje za obradu i pristup imaju isključivo radnici koji su za to ovlašteni u Službi naplate i obračuna utroška vode/Služba kontrole/Službi za pravne poslove i upravljanje ljudskim resursima.
Uvid u lične podatke	Uvid u lične podatke ima Rukovodilac službe naplate i obračuna utroška vode/ Šef odjeljenja naplate, Izvršni direktor za ekonomske i pravne poslove i Izvršni direktor za investicije i tehničke poslove. Dokumentacija iz arhive može se izdavati isključivo po nalogu nadležnih pravosudnih i inspekcijskih organa, na osnovu zahtjeva ovlašćenih lica unutar Preduzeća, po pismenom zahtjevu fizičkih lica na koje se podaci odnose, ukoliko postoji zakonski osnov i identitet je potvrđen, po zahtjevu drugih lica u postupku, uz prethodnu pravnu provjeru osnova zahtjeva.
Zabrana pristupa	Zabranjen je pristup ili obrada podataka od strane neovlaštenih lica, kao i svaka obrada izvan propisane

	svrhe.
Evidencije	Svi uvidi u lične podatke se evidentiraju u odgovarajućem zapisu ili sistemskom logu (ime i prezime korisnika, datum i vrijeme uvida, svrhu i obim obrade). Evidencija se vodi kontinuirano i čuva se u službi, te na zahtjev Službenika ili Agencije za zaštitu ličnih podataka u BiH, mora biti dostupna.
Čuvanje dokumentacije	Dokumentacija u papirnom obliku čuva se u zaključanim ormarima ili prostorijama sa kontrolisanim pristupom, dok se elektronski podaci čuvaju u informacionim sistemima. Podaci se čuvaju u skladu sa važećim propisima i internim aktima i u skladu sa Listom kategorija registraturne građe sa rokovima čuvanja.
Postupanje Službe naplate i obračuna utroška vode u slučaju povrede ličnih podataka	U slučaju saznanja ili sumnje da je došlo do povrede ličnih podataka zaprimljenih putem protokola, u službi će se poduzeti sljedeće mjere: **Hitno utvrđivanje incidenta** (odmah provjeriti da li je došlo do povrede, npr. neovlašten pristup, gubitak dokumenata, slanje podataka pogrešnom primatelju, objavljivanje, krađa uređaja i sl.; identifikovati koje kategorije podataka su kompromitovane i u kojem obimu). **Sprečavanje daljnje povrede** (ograničiti pristup kompromitovanoj evidenciji; osigurati dokumente ili uređaje koji su izloženi (zaključavanje, povlačenje kopija, vraćanje pogrešno poslanih dokumenata). **Dokumentovanje incidenta** Sačinjava se zapisnik koji sadrži: datum, vrijeme i opis incidenta, podatke koji su izloženi, osobe uključene u incident, hitne mjere koje su poduzete, procjenu rizika za prava i slobode osoba na koje se podaci odnose. **Obavještavanje Službenika za zaštitu podataka** Bez odlaganja obavještava se Službenik za zaštitu ličnih podataka - dostavljaju se sve dostupne informacije kao i zapisnik kako bi se mogla procijeniti ozbiljnost povrede i potreba za daljnjim koracima. **Procjena rizika** Rukovodilac službe za pravne poslove i upravljanje ljudskim resursima, Rukovodilac službe naplate i obračuna utroška vode i Šef odjeljenja IT i Službenik za zaštitu ličnih podataka daju ocjenu da li povreda predstavlja visok rizik po prava i slobode zaposlenika, da li postoji opasnost od finansijske štete, krađe identiteta, diskriminacije ili narušavanja privatnosti. **Obavještavanje nadležne Agencije** (Ako se utvrdi da povreda zahtijeva prijavu Službenik za zaštitu ličnih podataka obavještava Agenciju i dostavlja sačinjenu dokumentaciju). **Obavještavanje oštećenih** (Ako povreda može uzrokovati štetu radnicima i eksternim korisnicima

	potrebno ih je obavjestiti, jasno, razumljivo i bez odlaganja; dati informacije o vrsti povrede, mogućim posljedicama i preporukama za zaštitu). **Preduzimanje korektivnih mjera** (uklanjanje uzroka incidenta npr. izmjena procedura, pojačavanje pristupnih prava, brisanje pogrešno distribuiranih podataka; preventivne mjere).

Sažeto: *Radnik koji uoči ili posumnja na povredu ličnih podataka dužan je odmah obavijestiti šefa službe i rukovodioca sektora o nastalom "incidentu", a rukovodilac/šef službe bez odlaganja obavijestiti Službenika za zaštitu ličnih podataka, te dostaviti izvještaj o povredi putem e-pošte ili internog sistema.*

Službenik za zaštitu ličnih podataka dužan je potvrditi prijem prijave u roku od 24 sata, provjeriti njenu osnovanost te, u saradnji odjeljenjem IT i nadležnom službom, utvrditi vrstu i opseg povrede, pogođene podatke i lica, moguće posljedice, vjerovatnoću ponavljanja i nivo rizika (nizak, srednji ili visok).

U slučaju postojanja rizika po prava i slobode lica, Službenik je dužan obavijestiti Agenciju za zaštitu ličnih podataka u BiH u roku od 72 sata od saznanja za povredu, a nadležna služba pogođene nosioce ličnih podataka bez nepotrebnog odgađanja, jasnim i razumljivim jezikom.

Nadležna služba preduzima odgovarajuće tehničke i organizacione mjere radi otklanjanja uzroka povrede. Službenik za zaštitu ličnih podataka sačinjava konačan izvještaj o incidentu koji dostavlja Upravi na potpis, predlaže preventivne mjere, evidentira slučaj kao zatvoren i čuva kompletnu dokumentaciju najmanje pet godina.

Treća strana sumnju na povredu može prijaviti putem e-pošte na adresu (SZLP@viksa.ba) ili pismenim putem na adresu sjedišta Preduzeća.

Član 15.

(Prava nosilaca podataka)

(1) Nosilac podataka ima pravo na: pravo na pristup, ispravku, brisanje, ograničenje obrade, prigovor i obraćanje Agenciji.

(2) Nosilac podataka prava iz stava 1. ovog člana ostvaruje popunjavanjem *Zahtjeva nosioca podataka*, koji čini sastavni dio Pravilnika o provođenju odredaba Zakona o zaštiti ličnih podataka u KJKP „VIK" d.o.o. Sarajevo (*Prilog br. 2*), a učinit će se dostupnim i na web stranici Preduzeća.

(3) Preduzeće je dužno, na zahtjev nosioca podataka, u roku od 30 dana dostaviti informacije o obradi ličnih podataka. Rok se može produžiti uz obrazloženje. Informacije se dostavljaju u formi zahtjeva, a identitet nosioca provjerava Službenik za zaštitu ličnih podataka.

(4) Nosilac podataka ima pravo zahtijevati ispravku, dopunu ili brisanje netačnih, nepotpunih ili nezakonito obrađenih ličnih podataka, osim ako postoji zakonska obaveza njihovog čuvanja. Preduzeće osigurava transparentan postupak i obavještava nosioca o preduzetim radnjama

(5) Nosilac podataka ima pravo na ograničenje obrade u slučajevima osporavanja tačnosti, nezakonite obrade, pravnih zahtjeva ili uloženog prigovora. Preduzeće obavještava nosioca prije ukidanja ograničenja.

(6) Nosilac podataka ima pravo u svakom trenutku uložiti prigovor ako smatra da se lični podaci obrađuju suprotno Zakonu.

(7) Svi zahtjevi nosilaca podataka se evidentiraju u skladu sa Pravilnikom o provođenju odredaba Zakona o zaštiti ličnih podataka u KJKP „VIK" d.o.o. Sarajevo.

Član 16.

(Procjena rizika i uticaj na zaštitu ličnih podataka)

1) Preduzeće vrši procjenu rizika po sigurnost ličnih podataka prilikom uvođenja novih sistema, tehnologija ili značajnih promjena u načinu obrade ličnih podataka.
2) Kada je vjerovatno da određena obrada predstavlja visok rizik po prava i slobode lica, sprovodi se procjena uticaja na zaštitu ličnih podataka.
3) Službenik za zaštitu ličnih podataka učestvuje u izradi procjene i daje preporuke za smanjenje rizika.

Član 17.

(Obrada ličnih podataka putem obrađivača ili trećih lica)

1) Obrada ličnih podataka putem obrađivača ili trećih lica dozvoljena je isključivo na osnovu pisanog sporazuma o obradi i zaštiti ličnih podataka.
2) Sporazumom o obradi i zaštiti ličnih podataka uređuju se predmet i trajanje obrade, priroda i svrha obrade, vrste ličnih podataka, kao i obaveze i odgovornosti izvršioca obrade.
3) Obrađivači i treća lica su dužna primjenjivati iste ili više standarde zaštite ličnih podataka kao Preduzeće.
4) Izvršilac obrade ne smije angažovati podizvršioce bez prethodne saglasnosti Preduzeća.

Član 18.

(Informisanje i obuka zaposlenih)

1) Službenik za zaštitu ličnih podataka provodit će obuku izvršilaca obrade zbirki ličnih podataka koji dolaze u dodir sa ličnim podacima, u okviru koje će radnici biti upoznati sa pravilima i procedurama zaštite ličnih podataka u postupcima obrade, pohranjivanja i arhiviranja, s ciljem osiguranja da se u svakom trenutku održava dosljedno visok standard sigurnosti kod svih zaposlenih
2) Nakon prijema u radni odnos, a prije otpočinjanja obavljanja radnih dužnosti, svako lice koje će u okviru poslova i zadataka obrađivati lične podatke upoznaje se sa mjerama zaštite ličnih podataka.

Član 19.

(Nivo zaštite ličnih podataka tokom fizičkog prijenosa između službi i zaposlenih)

1) Lični podaci koji se prenose između organizacionih jedinica i zaposlenih obrađuju se uz povećani nivo zaštite, tako što se dokumenti koji sadrže lične podatke dostavljaju isključivo u zatvorenoj koverti ili zatvorenoj fascikli, jasno označenoj kao povjerljiva dokumentacija.
2) Pristup dokumentima imaju isključivo ovlaštena lica, a prenos se vrši na način koji onemogućava neovlašten uvid, gubitak, izmjenu ili zloupotrebu podataka.
   Dokumentacija se predaje direktno ovlaštenom primaocu ili se odlaže na sigurno mjesto do preuzimanja od strane ovlaštenog lica.

Član 20.
(Sprečavanje neovlaštenog umnožavanja, kopiranja i prepisivanja ličnih podataka)

Lične podatke mogu umnožavati, kopirati ili prepisivati samo lica koja su zadužena za obradu ličnih podataka u skladu sa potrebama obavljanja redovnih radnih zadataka.

Član 21.
(Uništavanje dokumenata)

1) Lični podaci se moraju uništavati na siguran i kontrolisan način, tako da se onemogući njihovo raspoznavanje, rekonstrukcija ili ponovna upotreba, te da dokument, nosač podataka ili drugi medij koji sadrži lične podatke ne može biti obnovljen niti vraćen u prvobitno stanje.
2) Direktor Preduzeća će odrediti Komisiju za uništavanje dokumenata koji sadrže lične podatke, te je ista dužna sačiniti zapisnik o uništavanju. Komisiju čine tri člana. Komisija će, nakon što sačini zapisnik, isti dostaviti direktoru na verifikaciju.

III - TEHNIČKE MJERE

Član 22.
(Mjere tehničke zaštite)

1) Preduzeće obezbjeđuje odgovarajuće mjere tehničke zaštite podataka, opreme i prostorija u kojima se vrši obrada ličnih podataka.
2) Tehničke mjere zaštite ličnih podataka, između ostalog, obuhvataju kontrolu pristupa prostorijama i opremi za obradu ličnih podatka, zaštitu od uništenja i oštećenja ličnih podataka i drugo.
3) Mjerama iz stava (1) ovoga člana štite se lični podaci koji se vode u pisanom i elektronskom obliku.

Član 23.
(Fizičke mjere zaštite prostorija i opreme u kojima se vrši obrada ličnih podataka)

1) Sve kancelarije u kojima se obrađuju i arhiviraju lični podaci, trebaju biti zaštićene odgovarajućim mjerama fizičke zaštite. Kod odlučivanja o stepenu potrebne fizičke zaštite, u obzir će se uzeti relevantni faktori kao što su:

    a) kategorija ličnih podataka;
    b) količina i oblik (štampane na papiru/ na medijima za kompjutersko pohranjivanje);
    c) osoblje koje obrađuje informacije;
    d) kako će se arhivirati informacije.

2 Mjere fizičke zaštite su tako osmišljene da:
    a) spriječe nedozvoljen ili nasilan upad od strane neovlaštenog lica;
    b) odvrate, spriječe i otkriju radnje neovlaštenog lica;

c) omoguće selekciju osoblja u pogledu pristupa ličnim podacima i
d) omoguće otkrivanje i postupanje u svim slučajevima ugrožavanja sigurnosti što je prije moguće.

Član 24.
(Fizički nadzor ulaza i izlaza)

1) Sistem nadzora treba da bude osmišljen tako da obezbjeđuje potpuni nadzor nad ulazom/izlazom lica u prostorije objekata Preduzeća, dozvoljava ulaz samo licima koji imaju odgovarajuće odobrenje za pristup prostorijama ili koji su zaposleni u Preduzeću.
2) Prije ulaska nezaposlenih lica u prostorije, izuzimajući lica koja ulaze u centre za kupce, radnik ili drugo ovlašteno lice koje obavlja poslove zaštite Preduzeća mora provjeriti njihov identitet i razlog ulaska.
3) Nezaposlenim licima kojima se dozvoljava ulazak u prostorije Preduzeća izdaje se propusnica kojom se dozvoljava kretanje u prostorijama Preduzeća.
4) Sva lica koja nisu radnici Preduzeća, a koji posjećuju prostorije Preduzeća, moraju imati na vidljivom mjestu zakačenu akreditaciju za ulazak i kretanje kroz prostorije Preduzeća, a radnici i ovlaštena lica koja rade na poslovima zaštite u Preduzeću će voditi evidenciju o izdatim propusnicama.
5) Pristup prostorijama gdje se čuvaju i obrađuju lični podaci moguć je samo u toku redovnog radnog vremena. Izvan radnog vremena pristup takvim prostorijama je moguć samo zaposlenim licima prilikom obavljanja vanrednih službenih dužnosti uz dozvolu za boravak radnika izdatu od ovlaštenog lica u Preduzeću.

Član 25.
(Prostorije, ormari i kase)

1) Prostorije u kojima se obrađuju lični podaci, ne smiju ostajati bez nadzora radnika.
2) Zbirke ličnih podataka, koje se vode u pisanom obliku, pohranjuju se u uredskim ili metalnim ormarima i kasama.
3) Izvan radnog vremena, ormari i pisaći stolovi sa dokumentima koja sadrže lične podatke, moraju biti zaključani a računari i druga mašinska oprema isključeni i fizički ili programski zaključani.
4) Nije dozvoljeno ostavljati nosače ličnih podataka na stolovima u prisutnosti lica koja nemaju prava na pristup ili uvid tim podacima.
5) U prostorijama za rad sa strankama, dokumenti koji sadrže lične podatke i računarski monitori moraju biti postavljeni tako, da stranke ne mogu ostvariti uvid u iste.

Član 26.
(Video nadzor)

1) Službeni ulazi poslovnih objekata Preduzeća su pokriveni sistemom video nadzora.
2) Sistem video nadzora povezan je dojavnim operativnim centrom Preduzeća u kojem se 24 h primaju, obrađuju i prosljeđuju podaci primljeni putem sistema video nadzora. Sistem

videonadzora ima mogućnost arhiviranja podataka, kako bi se podaci mogli prikazati u slučaju da se za tim ukaže potreba.

3) Izvršilac zbirke ličnih podataka je zadužen za redovno pohranjivanje video zapisa na prenosive medije, te njihovo arhiviranje, zaštitu od neovlaštenog brisanja, te izuzimanje određenih dijelova snimaka, ukoliko se za tim ukaže potreba, uz saglasnost odgovornog lica za fizičku i tehničku zaštitu i direktora Preduzeća.

Član 27.

(Ključevi i kombinacije)

1) Ključevi prostorija u kojima se nalaze lični podaci, čuvaju se i upotrebljavaju u skladu sa utvrđenim pravilima.
2) Nije dozvoljeno ostavljanje ključeva u bravi sa vanjske strane vrata prostorije u kojoj se vrši obrada ličnih podataka.
3) Ključevi kancelarija u kojima se obrađuju lični podaci može imati samo izvršilac obrade ličnih podataka, a rezervni će se čuvati u prostorijama prijavnice objekta, a mogućnost njihovog korištenja je ograničena za potrebe obrade ličnih podataka, za potrebe osoblja koje vrši poslove higijenskog održavanja prostorija, odnosno u slučaju vandrednih situacija i krajnje nužde.
4) Pristupne šifre na metalnim kasama na blagajnama bit će poznate samo ovlaštenim radnicima.

Član 28.

(Posebne mjere zaštite)

1) U blizini računarske i telekomunikacione opreme ne smije biti izvora jakog električnog ili magnetskog polja i izvora jonizirajućeg zračenja.
2) U blizini opreme osjetljive na elektrostatički elektricitet ne smije biti izvora takvog elektriciteta.
3) U prostorijama i u blizini prostorija u kojima je smještena oprema sistema, ne smiju se nalaziti nagrizajuće tekućine, eksplozivna sredstva i slične opasne ili štetne materije.
4) U prostorijama u kojima su smješteni računari ne smiju se nalaziti uređaji koji u zrak ispuštaju čestice prašine. Uređaji osjetljivi na prašinu moraju biti propisno zaštićeni. Posebno osjetljivi uređaji koji se hlade zrakom, moraju imati filtere za zrak.

Član 29.

(Zaštita ličnih podataka u automatskoj obradi)

1) Preduzeće pri automatskoj obradi ličnih podataka obezbjeđuje tehničke mjere zaštite ličnih podatka i to:
    a) jedinstveno korisničko ime i lozinku za prijavu na elektronske evidencije sastavljenu od obavezne kombinacije minimum šest karaktera, brojeva ili slova;
    b) izmjenu lozinke po utvrđenom vremenskom periodu koji ne može biti duži od tri mjeseca;
    c) korisničko ime i lozinka će dozvoljavati pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka;

d) automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne duže od 15 minuta, a za ponovno aktiviranje sistema potrebno je nanovo upisati korisničko ime i lozinku;
e) efikasnu i sigurnu antivirusnu zaštitu sistema, koje će se stalno ažurirati radi preventive od nepoznate ili neplanirane opasnosti od novih virusa;
f) kompjuterska, programska i ostala neophodna oprema na elektorenergetsku mrežu se priključuje putem uređaja za neprekidno napajanje.

2) Služba za pravne poslove i upravljanje ljudskim resursima dužna je da izvještava Odjeljenje IT o zaposlenju ili angažovanju svakog izvršioca s pravom pristupa informacionom sistemu, kako bi se dodijelili korisničko ime i lozinka, kao i po prestanku zaposlenja ili angažovanja, da bi se korisničko ime i lozinka izbrisali odnosno zabranio daljnji pristup.
3) Izvještavanje iz stava (2) ovog člana vrši se i prilikom bilo koje druge promjene radnog statusa izvršioca, koja utiče na nivo ili obim pristupu zbirke ličnih podataka.

Član 30.
(Korisničko ime i lozinka)

1) Da bi korisnik pristupio informacionom sistemu Preduzeća potrebno je da ima važeći korisnički nalog i lozinku.
2) Svaki korisnik dobija korisnički nalog i početnu lozinku, koju je dužan promijeniti nakon prvog prijavljivanja na sistem.
3) Korisnički nalog je jedinstven i jedan korisnik može imati samo jedan korisnički nalog.

Član 31.
(Korisnička lozinka)

1) Korisnička lozinka treba da sadrži najmanje 6 (šest) karaktera, koji predstavljaju kombinaciju velikih i malih slova, te brojeva.
2) Korisnik je dužan mijenjati lozinku svakih 90 dana i ne smije je dijeliti sa drugim licima.
3) Lozinka ne smije sadržavati ime ili prezime korisnika ili bilo koji drugi podatak koji se na očigledan način mogu dovesti u vezu sa korisnikom.
4) Radnik je dužan da pamti svoju lozinku i ista se ne može zapisivati u blizini računara.
5) U slučaju da korisnik zaboravi svoju lozinku potrebno je da putem rukovodioca osnovne organizacione jedinice obavijesti Odjeljenje IT za dodjelu nove.

Član 32.
(Pristup sistemu)

Korisničko ime i lozinka će dozvoljavati pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka - privilegovani nivo.

Član 33.
(Automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti)

1) Kada se korisnici udaljavaju od računara, dužni su obavezno da se odjave sa sistema.
2) Obavezno je automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne duže od 15 minuta. Za ponovno aktiviranje sistema potrebno je ponovo upisati korisničko ime i lozinku.

Član 34.

(Antivirusna zaštita)

Informacioni sistem Preduzeća mora imati efikasnu i sigurnu antivirusnu zaštitu sistema, koja se redovno ažurira radi preventive od nepoznate ili neplanirane opasnosti od novih virusa.

Član 35.

(Obaveza upotrebe uređaja za neprekidno napajanje)

Računari za vođenje zbirki ličnih podataka i njegovo mrežno čvorište se priključuju na energetsku mrežu preko uređaja za neprekidno napajanje (UPS).

Član 36.

(Dodatne mjere)

Preduzeće pri automatskoj obradi ličnih podataka obezbjeđuje:

a) potpunu tajnost i sigurnost lozinki i ostalih formi za identifikaciju pristupa ličnim podacima;
b) uništavanje medija koji sadrže lične podatke po isteku roka za obradu;
c) svako iznošenje bilo kojeg medija koji sadrži lične podatke van radnih prostorija mora biti sa posebnom dozvolom i kontrolom da ne dođe do gubljenja ili nezakonitog korištenja;
d) poštivanje tehničkih uputstava pri instaliranju i korištenju opreme koja služi za obradu ličnih podataka.

Član 37.

(Tajnost lozinki)

Preduzeće će osigurati potpunu tajnost lozinki i ostalih načina pristupa računarima i programima na kojima se vrši obrada ličnih podataka.

Član 38.

(Iznošenje ličnih podataka van radnih prostorija)

1) Mediji koji sadrže lične podatke, mogu se iznositi van radnih prostorija samo uz posebnu dozvolu koju izdaje direktor Preduzeća, odnosno lica koje direktor ovlasti.
2) Radnik koji iznosi medij koji sadrži lične podatke dužan je obezbjediti iste kako ne bi došlo do gubljenja ili nezakonitog korištenja medija koji se iznosi.

Član 39.

(Pristup server prostoriji)

1) Server prostorije su smještene na dvije lokacije, klimatizovane su sa adekvatnim uzemljenjem.
2) U prostoriji iz stava 1. nalaze se serveri koji su fizički odvojeni od ostalih prostorija.
3) Prostorija u kojoj su smješteni serveri mora imati jedan od pristupnih sigurnosno-zaštitnih mehanizama na ulaznim vratima.
4) Fizički pristup server prostoriji dozvoljen je samo ovlaštenim radnicima: Odjeljenja IT.

5) Izuzetno, ulaz u server prostoriju dozvoljen je u vandrednim situacijama (požar, poplava ili neka druga elementarna nepogoda) i to samo licima koja su nadležna da postupaju u takvim situacijama.

Član 40.

(Smještanje, postavljanje i ugradnja računara i računarske mreže)

Računari za vođenje zbirki ličnih podataka, centralni računar zbirki i računarsku mrežu smješta, postavlja i ugrađuje stručna osoba, u skladu s važećim normama, standardima i tehničkim uputstvima.

Član 41.

(Poštovanje tehničkih uputstava pri instaliranju i korištenju opreme za obradu ličnih podataka)

1) Na svim uređajima za obradu ličnih podataka su instalirani softveri u skladu sa potrebama radnih procesa.
2) Nije dozvoljeno instaliranje i korištenje softvera koji nemaju licencu i koji nisu odobreni od strane Odjeljenja IT.
3) Instalaciju softvera kao i sve zamjene na postojećoj opremi za obradu ličnih podataka vrši Odjeljenje IT ili treća lica koja imaju važeći ugovor ili odobrenje.
4) Održavanje i popravljanje mašinske, informatičke i druge opreme mogu izvoditi samo ovlašteni radnici Odjeljenja IT ili ovlašteni servisi, u skladu sa ugovorom o održavanju koji je potpisan između Preduzeća i ovlaštenog servisera.
5)

Član 42.

(Brisanje podataka pri automatskoj obradi)

1) Po isteku roka čuvanja, lični podaci se brišu, uništavaju i blokiraju, osim ukoliko nije drugačije određeno.
2) Prenos nosača podataka na mjesto uništenja, te uništavanje nosača ličnih podataka nadzire posebna komisija, koja sastavlja odgovarajući zapisnik o uništenju.

Član 43.

(Mrežna barijera)

Preduzeće obezbjeđuje odgovarajuću zaštitu - mrežnu barijeru između informacionog sistema i Internet mreže, ili bilo koje druge forme spoljne mreže, kao zaštitu protiv nedozvoljenog pokušaja ulaza u sistem.

Član 44.

(Pravo pristupa sistemu za vođenje evidencija)

1) Pristup podacima pohranjenim u evidencijama ličnih podataka, pored izvršioca obrade dozvoljen je isključivo ovlaštenim licima, u skladu sa jasno definisanim obavezama i odgovornostima utvrđenim od strane Preduzeća, isključivo u svrhu uvida i kontrole zakonitosti obrade ličnih podataka, te u skladu sa važećim zakonom i internim aktima Preduzeća.

2) Direktor Preduzeća, odnosno član Uprave kojeg ovlasti, određuje ovlaštena lica za uvid i kontrolu zbirki ličnih podataka.

Član 45.

(Evidencija, praćenje pristupa i pokušaj neovlaštenog pristupa sistemu)

Svaki pristup informacionom sistemu za vođenje evidencija ličnih podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave.

Član 46.

(Sigurnosna kopija)

1) Odjeljenje IT vrši redovno snimanje sigurnosnih kopija ili arhiviranje podataka u sistemu, da ne bi došlo do njihovog gubljenja ili uništenja.
2) Svaki primjerak pohranjenih podataka na prenosivom informatičkom mediju mora biti označen brojem, vrstom, datumom pohranjivanja.
3) Prije ili istovremeno sa zaključivanjem ugovora iz prethodnog stava, Preduzeće je obavezno da sa pružaocem usluga zaključi poseban sporazum o zaštiti ličnih podataka, kojim se uređuju prava i obaveze ugovornih strana u vezi sa obradom, čuvanjem i zaštitom ličnih podataka, u skladu sa važećim propisima.

Član 47.

(Zaštita posebne kategorije ličnih podataka)

1) Prilikom obrade posebne kategorije ličnih podataka u svim fazama obrade, Preduzeće označava da se radi o obradi navedene kategorije podataka;
2) Preduzeće preduzima dopunske tehničke, organizacione mjere pri obradi posebnih kategorija ličnih podataka;
3) Putem dopunskih tehničkih i organizacionih mjera pri obradi posebne kategorije ličnih podataka obezbjeđuje se:
    a. mogućnost za prepoznavanje svakog pojedinačnog ovlaštenog pristupa informacionom sistemu;
    b. rad sa podacima posebne kategorije ličnih podataka vrši se isključivo tokom redovnog radnog vremena Preduzeća. Izuzetno se posebni podaci mogu obrađivati i van radnog vremena o čemu mora biti obaviješten rukovodilac organizacione jedinice gdje se vrši obrada ličnih podataka;
4) Radi pravilnog postupanja s dokumentacijom o privremenoj spriječenosti za rad (bolovanje) te
zaštite posebne kategorije ličnih podataka, utvrđuje se sljedeći način postupanja:
5) Radnik je obvezan obavijest o otvaranju bolovanja, koju izdaje nadležna zdravstvena ustanova, dostaviti u zatvorenoj omotnici Službi za računovodstvo i finansije/Referentu za obračun plaća

Nakon zaprimanja obavijesti o bolovanju, u službi se sačinjava informacija koja se putem

e-maila dostavlja šefu službe, sa naznakom da je određeni radnik otvorio bolovanje.

Član 48.

(Rokovi čuvanja i brisanje ličnih podataka)

1) Lični podaci se čuvaju samo onoliko dugo koliko je neophodno za ostvarivanje svrhe obrade ili u skladu sa zakonskim obavezama.
2) Po isteku roka čuvanja, podaci se brišu, anonimizuju ili arhiviraju u skladu sa propisima.

3) Brisanje podataka mora biti izvršeno na način koji onemogućava njihovu obnovu.

V – ZAVRŠNE ODREDBE

Član 49.
(Obaveze organizacionih jedinica u primjeni mjera zaštite ličnih podataka i procjeni uticaja obrade)

1) Svaka organizaciona jedinica u okviru Preduzeća, putem svog rukovodioca, odnosno šefa službe/odjela, dužna je da planira, uspostavi i primjenjuje odgovarajuće tehničke i organizacione mjere radi obezbjeđivanja sigurnosti, integriteta i povjerljivosti obrade ličnih podataka, u skladu sa važećim propisima i ovim Planom sigurnosti.
2) Ukoliko je vjerovatno da će određena vrsta obrade ličnih podataka, naročito kada uključuje primjenu novih tehnologija, uzimajući u obzir prirodu, obim, kontekst i svrhu obrade, predstavljati visok rizik za prava i slobode fizičkih lica, nadležne organizacione jedinice dužne su da prije započinjanja obrade provedu procjenu uticaja na zaštitu ličnih podataka (DPIA), u skladu sa važećim propisima.
3)

Član 50.
(Odgovornost za provođenje mjera obezbjeđenja ličnih podataka)

1) Za provođenje postupaka i mjera zaštite ličnih podataka odgovorni su rukovodioci i šefovi organizacionih jedinica, u skladu sa nadležnostima i odgovornostima iz organizacionih jedinica.
2) Za primjenu mjera obezbjeđenja, pohranjivanja i zaštite ličnih podataka koje se obrađuju i vode u pisanom i elektronskom obliku odgovarni su radnici koji su ovlašteni u skladu sa ovim Planom.
3) Svako, ko obrađuje lične podatke, dužan je sprovoditi propisane postupke i mjere za zaštitu ličnih podataka, za koje je saznao odnosno bio upoznat sa njima prilikom izvršavanja svojih obaveza.
4) Obaveza čuvanja podataka ne prestaje sa prestankom radnog odnosa.

Član 51.
(Zloupotreba ličnih podataka)

Sa svakim neovlaštenim pristupom ličnim podacima, njihovim uništenjem, krađom ili drugim događajem koji ukazuje na zloupotrebu ličnih podataka, treba odmah upoznati direktora Preduzeća odnosno Službenika za zaštitu ličnih podataka i obezbjediti sve mjere za onemogućavanje dalje zloupotrebe ličnog podatka, te provesti istragu o okolnostima zloupotrebe.

Član 52.
(Disciplinska odgovornost)

Svi radnici su disciplinski odgovorni za kršenje odredbi ovog Plana.

Član 53.
(Usklađivanje)

Preduzeće je obavezno u roku od godinu dana od stupanja na snagu ovog Plana uskladiti mjere, sredstva i uslove osiguranja, pohranjivanja i zaštite podataka sa odredbama ovog akta.

Član 54.
(Revizija i ažuriranje Plana)

1) Ovaj Plan se redovno preispituje, a najmanje jednom u dvije godine
2) Plan se ažurira u slučaju izmjena propisa, uvođenja novih informaconih sistema ili promjena u načinu obrade ličnih podataka.

Član 55.
(Stupanje na snagu)

Ovaj Plan stupa na snagu dana 18.05.2026. godine, a biće objavljen na oglasnim pločama Preduzeća i intranet stranici Preduzeća.

Broj: 3684/1
Datum: 18.05.2026. godine

KANTONALNO JAVNO KOMUNALNO PREDUZEĆE VODOVOD I KANALIZACIJA D.O.O. SARAJEVO

Direktor

Adnan Šerak