PRAVILNIK ZA ZAŠTITU OSOBNIH PODATAKA

Datum 5.6.2023.

Odobrila: Sunčica Brajković, direktor

Sadržaj

DEFINICIJE POJMOVA

Pojam	Definicija
Ispitanici	Pojedinci ili fizičke osobe čiji se osobni podaci obrađuju. To su zaposlenici i korisnici usluge te ostale zainteresirane strane ukoliko one postoje.
Osobni podaci	„osobni podaci" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.
Obrada	„obrada" znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.
Ograničavanje obrade	„ograničavanje obrade" znači označivanje pohranjenih osobnih podataka s ciljem ograničavanja njihove obrade u budućnosti.
Izrada profila	„izrada profila" znači svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.
Pseudonimizacija	„pseudonimizacija" znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.
Sustav pohrane	„sustav pohrane" znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.
Voditelj obrade	„voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice.
Izvršitelj obrade	„izvršitelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.
Primatelj	„primatelj" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade.
Treća strana	„treća strana" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade.
Privola	„privola" ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.
Povreda osobnih	„povreda osobnih podataka" znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog

podataka	uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.
Genetski podaci	„genetski podaci" znači osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca.
Biometrijski podaci	„biometrijski podaci" znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.
Podaci koji se odnose na zdravlje	„podaci koji se odnose na zdravlje" znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu.
Glavni poslovni nastan	„glavni poslovni nastan" znači: (a) što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u Uniji, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u Uniji te je potonji poslovni nastan ovlašten provoditi takve odluke, u kojem seslučaju poslovni nastan u okviru kojeg se donose takve odluke treba smatrati glavnim poslovnim nastanom; (b) što se tiče izvršitelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u Uniji, ili, ako izvršitelj obradenema središnju upravu u Uniji, poslovni nastan izvršitelja obrade u Uniji u kojem se odvijaju glavne aktivnosti obrade u kontekstu aktivnosti poslovnog nastana izvršitelja obrade u mjeri u kojoj izvršitelj obrade podliježe posebnim obvezama u skladu s ovom Uredbom.
Predstavnik	„predstavnik" znači fizička ili pravna osoba s poslovnim nastanom u Uniji koju je voditelj obrade ili izvršitelj obrade imenovao pisanim putem u skladu s člankom 27., a koja predstavlja voditelja obrade ili izvršitelja obrade u pogledu njihovih obveza na temelju ove Uredbe.
Poduzeće	„poduzeće" znači fizička ili pravna osoba koja se bavi gospodarskom djelatnošću, bez obzira na pravni oblik te djelatnosti, uključujući partnerstva ili udruženja koja se redovno bave gospodarskom djelatnošću.
Grupa poduzetnika	„grupa poduzetnika" znači poduzetnik u vladajućem položaju te njemu podređeni poduzetnici.
Obvezujuća korporativna pravila	„obvezujuća korporativna pravila" znači politike zaštite osobnih podataka kojih se voditelj obrade ili izvršitelj obrade s poslovnim nastanom na državnom području države članice pridržava za prijenose ili skupove prijenosa osobnih podataka voditelju obrade ili izvršitelju obrade u jednoj ili više trećih zemalja unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću.
Nadzorni tijelo	„nadzorno tijelo" znači neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51.
Predmetno nadzorno tijelo	„predmetno nadzorno tijelo" znači nadzorno tijelo koje je povezano s obradom osobnih podataka zato što: (a) voditelj obrade ili izvršitelj obrade ima poslovni nastan na državnom području države članice tog nadzornog tijela; (b obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela; ili (c) podnesena je pritužba tom nadzornom tijelu.

Prekogranična obrada	„prekogranična obrada” znači ili: (a) obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti poslovnih nastana u više od jedne države članice voditelja obrade ili izvršitelja obrade, a voditelj obrade ili izvršitelj obrade ima poslovni nastan u više od jedne države članice; ili (b) obrada osobnih podataka koja se odvija u Uniji u kontekstu aktivnosti jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade, ali koja bitno utječe ili je izgledno da će bitno utjecati na ispitanike u više od jedne države članice.
Relevantni i obrazloženi prigovor	„relevantni i obrazloženi prigovor” znači prigovor na nacrt odluke kao i na to je li došlo do kršenja ove Uredbe, ili je li djelovanje predviđeno u vezi s jasno pokazuje važnost rizika koje predstavlja nacrt odluke u pogledu temeljnih prava i sloboda ispitanika i, ako je primjenjivo, slobodnog protoka osobnih podataka unutar Unije.
Usluga informacijskog društva	„usluga informacijskog društva” znači usluga kako je definirana člankom 1. stavkom 1. točkom 2. Direktive 2015/1535 Europskog parlamenta i Vijeća.
Međunarodna organizacija	„međunarodna organizacija” znači organizacija i njezina podređena tijela uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na osnovi sporazuma osnovale dvije ili više zemalja.
Tehničko organizacijske mjere zaštite (TOM-ovi)	Mjere koje je voditelj obrade osobnih podataka uspostavio unutar svoje organizacije a koje za cilj imaju smanjivanje rizika povezanih s obradom osobnih podataka.
Procedure (prava postupanja)	Opisana prava i način postupanja u ispunjavanju zahtjeva ispitanika, a koji su povezani s obradom njegovih osobnih podataka.

1. UVOD

Svrha ovog Pravilnika je donošenje internog akta koji će potvrditi opredijeljenost Komunalnog Ozalj d.o.o. za sustav upravljanja zaštite osobnih podataka prema GDPR uredbi.

Zainteresiranim stranama će omogućiti sistematizirani pregled načina postizanja zaštite osobnih podataka u našoj organizaciji. Zainteresirane strane su naši zaposlenici, vodstvo, korisnici usluge, dobavljači, partneri ili nadležno nadzorno tijelo kao što je Agencija za zaštitu osobnih podataka.

Zaštita osobnih podataka je postala dio naše poslovne politike. Svjesni smo da prihvaćanjem načela i zahtjeva koje GDPR uredba propisuje, štitimo i provodimo temeljno pravo klijenata na zaštitu njegovih osobnih podataka. Unutar Komunalnog Ozalj d.o.o. proveli smo analizu osobnih podataka, procijenili potencijalne rizike, usvojili određene zaštitne mjere organizacijskog i tehničkog karaktera, uspostavili smo procedure, vodimo evidencije, prema zainteresiranim stranama smo zahtijevali privole tamo gdje su bile potrebne.

Komunalno Ozalj d.o.o. je postavila zaštitu osobnih podataka korisnika usluge kao jedan od najviših ciljeva upravljanja. Pravilnik za zaštitu osobnih podataka i sustavno izgrađena dokumentacija nedvosmisleno potvrđuju da smo poduzeli sve aktivnosti kako bi smanjili mogućnost nastanka rizika za osobne podatke klijenata.

Nijedna organizacija danas ne može uspješno poslovati bez razmjene informacija (podataka). Protok tih informacija (podataka) ide u svim smjerovima: između poslovnih subjekata, između fizičkih osoba, podaci se razmjenjuju i između kontinenata. Obradu podataka vrše javne institucije, udruge, klubovi, stranke odnosno svi bez obzira na organizacijsko obilježje i status.

Obrada tih podataka je važan segment funkcioniranja gospodarstva. U informacijskim razmjenama vrlo često dolazi do povrede osobnih podataka. Smatramo da će GDPR uredba upravo pridonijeti stvaranju kulture zaštite osobnih podataka. Komunalno Ozalj d.o.o. će svakako biti važan partner promicanju zaštite osobnih podataka unutar naše organizacije ali i prema van.

Komunalno Ozalj d.o.o. je uspostavio uskladio te kontinuirano nadzire i poboljšava sustav upravljanja zaštitom osobnih podataka prema GDPR uredbi.

1.1. Svrha

Svrha zaštite osobnih podataka je da našim zaposlenicima, korisnicima usluge i ostalim zainteresiranim stranama pružimo pouzdane informacije o uspostavljenom Sustavu upravljanja zaštite osobnih podataka koji se temelji na GDPR uredbi.

Svaka obrada osobnih podataka trebala bi biti zakonita i poštena. Za klijente usluga i zaposlenike bi trebalo biti transparentno kako se osobni podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podaci obrađuju ili će se obrađivati.

Osobne podatke trebalo bi obrađivati uz odgovarajuće poštovanje sigurnosti i povjerljivosti osobnih podataka, što obuhvaća i sprečavanje neovlaštenog pristupa osobnim podacima i opremi (računala) koja se koristi pri obradi podataka ili njihove neovlaštene upotrebe.

1.2. Upravljanje Pravilnikom

Pravilnikom za zaštitu osobnih podataka prema GDPR uredbi se upravlja na način da ga se pregledava, mijenja, odobrava i distribuira u nadziranim uvjetima.

Pravilnik objavljujemo kao original u elektronskoj formi na računalu.

1.3. Područje primjene Pravilnika

Područje primjene se odnosi na osobne podatke koje obrađujemo u našem poslovanju. Osobni podaci su svi oni koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podacima o lokaciji, mrežnim identifikatorom ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

2. O Nama

2.1.1. Osnovni podaci:

Komunalno Ozalj d.o.o.

Ulica Akademika Milana Heraka 11, Ozalj
OIB: 05352816122

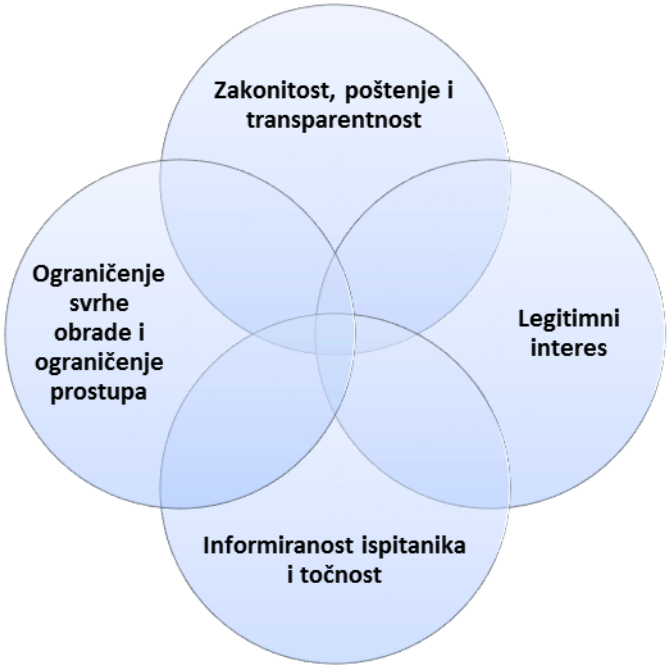
2.1.2. Djelatnost

Glavna djelatnost Komunalnog Ozalj-a d.o.o. je sakupljanje, pročišćavanje i opskrba vodom.

2.1.3. Načela zaštite osobnih podatka

Komunalno Ozalj d.o.o. je prihvatio sljedeća načela zaštite osobnih podataka koja će asimilirati u svoju postojeću organizacijsku kulturu:

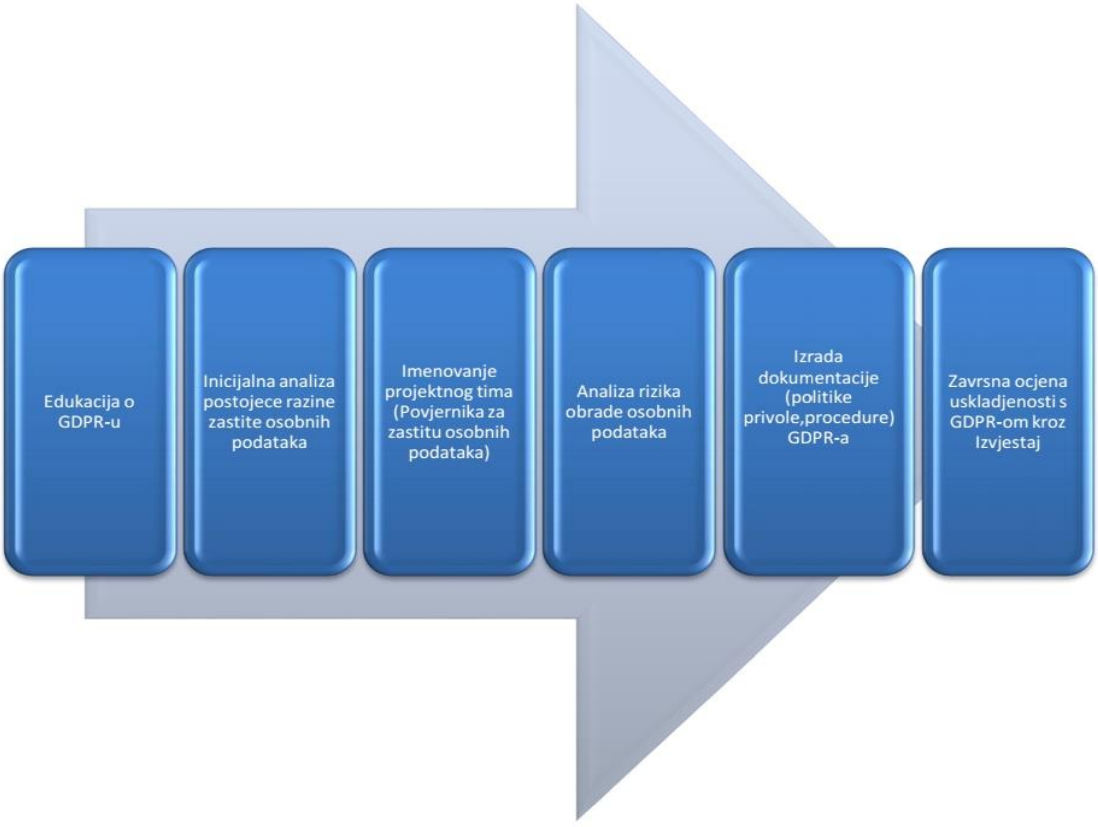
1. Obrada podataka će sadržavati načela zakonitosti, poštenja i transparentnosti obrade. Obrada podataka se mora vrši u legitimnu svrhu, uz adekvatnu informiranost zaposlenika.
2. Obrada podataka podrazumijeva ograničavanje svrhe radi koje se podaci obrađuju.
3. Podaci koji se obrađuju moraju biti prilagođeni svrsi (ograničeni,relevantni) u koju se obrađuju.
4. Poduzimamo sve mjere kako bi se osigurala točnost podataka koji se obrađuju.
5. Podaci su adekvatno pohranjeni u obliku koji omogućuje identifikaciju ispitanika kroz potrebito vremensko razdoblje dok traje obrada. Podatke čuvamo i duže ako se obrada radi u svrhe javnih, znanstvenih, statističkih ispitivanja.
6. Podaci su osigurani od neovlaštene ili nezakonite obrade te slučajnog gubitka ili uništenja.
7. Odgovorni smo za poštivanje i ispunjavanje svih načela obrade podataka.



Slika 1.: Prikaz usvojenih načela poslovanja vezanih za zaštitu osobnih podataka

2.1.4. **Projekt uvođenja i usklađivanja s GDPR uredbom**

Komunalno Ozalj d.o.o. kako bi što efikasnije uvelo i uskladio se s GDPR uredbom, definirala je projektni pristup. Projektni pristup se sastojao od 6 faza. Sve identificirane faze su slijedne i međuovisne.



Slika 2. : Faze uvođenja i usklađivanja s GDPR uredbom

Projekt uvođenja i usklađivanja s GDPR uredbom se sastojao od sljedećih faza:

1. Edukacija o GDPR uredbi za zaštitu osobnih podataka.

• Upoznavanje s osnovnim terminima (osobni podatak, ispitanik, voditelj i izvršitelj obrade, službenik, načela, privole te ostalom terminologijom Uredbe)
• Upoznavanje sa zahtjevima Uredbe i obvezama Voditelja obrade
• Razumijevanje GDPR-a s primjerima iz prakse

2. Imenovanje projektnog tima za provedbu GDPR-a.

• Sastavljanje tima koji će biti uključen u Projekt
• Imenovanje Službenika (povjerenika) za zaštitu osobnih podataka
• Definiranje obveza i odgovornosti

3. Inicijalna analiza podataka s kojima organizacija raspolaže.

• Analiza kategorija osobnih podataka

• Analiza postojećeg sustava zaštite osobnih podataka
• GAP analiza postojećeg sustava od zahtijevanog iz Uredbe

4. Klasifikacija podataka i procjena učinaka

• Procjene rizika kojima se izlažu podatci u poslovanju
• Definiranje organizacijskih i tehničkih mjera za zaštitu osobnih podataka

5. Izrada GDPR dokumentacije prema zahtjevima Uredbe

• Politika zaštite osobnih podataka i imenovanja
• Izrada procedura, Izvještavanje AZOP-a, procedure ostvarivanje prava ispitanika i podnošenja pritužbi, procedure za korištenje, dijeljenje, obradu i zaštitu osobnih podataka, procedure prava na brisanje podataka, na upit o obradi, pravo na prijenos podataka te sve ostale procedure koje Uredba zahtjeva
• Izrada evidencije edukacije, evidencije aktivnosti obrade osobnih podataka, evidencije aktivnosti ostvarivanja prava ispitanika te sve ostale evidencije
• Izrada radnih uputa, zapisa, privola, mjera zaštite
• Izrada Pravilnika zaštite osobnih podataka
• Izrada ostale dokumentacije prema potrebi poslovanja organizacije

6. Završna ocjena razine usklađenosti s GDPR uredbom kroz sastavljanje Izvještaja.

• Objektivan i neovisan Izvještaj o provedenim mjerama usklađenosti s GDPR uredbom te prijedlozima poboljšanja

2.1.5. **Imenovanje Službenika za zaštitu osobnih podataka**

Imenovanje Službenika za zaštitu podataka temelji se na članku 37. Uredbe o zaštiti osobnih podataka – GDPR (Gemeral Data Protection Regulation).

Službenik za zaštitu osobnih podataka u Komunalnom Ozalj d.o.o. je Ljiljana Lukunić.

Službenik, gđa. Ljiljana Lukunić je upoznata sa svojim pravima i obvezama koje iz takvog imenovanja proizlaze. U to ime izrađena su dva dokumenta: *Imenovanje službenika za zaštitu osobnih podataka i Izjava službenika za zaštitu osobnih podataka.* Jedan dokument je formalno imenovanje, a drugi prihvaćanje obveza i odgovornosti za zaštitu osobnih podataka.

Glavne zadaće Službenika za zaštitu osobnih podataka su:

1. Izvještavanje Uprave o efikasnosti i promjenama u sustavu upravljanja zaštitom osobnih podataka prema GDPR uredbi.
2. Vođenje evidencija i ažuriranje GDPR dokumentacije.
3. Čuvanje GDPR dokumentacije elektronički ili papirno u uredskom ormariću ili ladici pod ključem.
4. Promicanje i provedba tehničkih i organizacijskih mjera za postizanje zaštite osobnih podataka odnosno umanjenja rizika povezanih s istim.

5. Periodični pregled, ispitivanje i ocjena sustava upravljanja zaštite osobnih podataka kroz Interni audit.

6. Prepoznavanje znakovitih tehnoloških trendova koje mogu utjecati na sustav upravljanja zaštite osobnih podataka.
7. Praćenje zakonskih izmjena i smjernica povezanih sa sustavom upravljanja zaštite osobnih podataka prema GDPR uredbi.
8. Komunikacija s ispitanicima i djelovanje prema procedurama GDPR dokumentacije.
9. Komunikacija s nadležnim nadzornim tijelom Agencijom za zaštitu osobnih podataka.
10. Koordinacija i dijeljenje radnih uputa GDPR dokumentacije unutar organizacije.
11. Pružanje podrške istragama povezanih s povredama zaštite osobnih podataka.
12. Podizanje ukupne svijesti unutar organizacije o potrebi zaštite osobnih podataka svih ispitanika (pojedinaca).

2.1.6. **Politika zaštite osobnih podataka**

Politika zaštite osobnih podataka je dokument kojeg Komunalno Ozalj d.o.o. objavljuje deklarativno prema svim zainteresiranim stranama odnosno ispitanicima. Na takav način želimo skrenuti pozornost važnosti zaštite osobnih podataka prema našim zaposlenicima, korisnicima usluge, dobavljačima i partnerima.

Smatramo da su osobni podatci povezani s temeljnim pravom i slobodom svakog pojedinca što je definirano i člankom 8. stavkom 1. Povelje Europske unije o temeljnim pravima te člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije gdje se utvrđuje da svatko ima pravo na zaštitu svojih osobnih podataka.

Komunalno Ozalj d.o.o. želi obavijestiti sve zainteresirane strane (korisnike usluge, dobavljače, poslovne partnere, zaposlenike, zakonodavca) da smo usklađeni s temeljnim načelima obrade osobnih podataka iz Uredbe o zaštiti osobnih podataka članak 5. stavak 1.

U to ime proveli smo čitav niz aktivnosti kako bi demonstrirali pouzdanost i dokazivost prema GDPR uredbi. Imenovali smo Službenika za obradu osobnih podataka, izradili smo procedure za zaštitu podataka, prepoznali potencijalne rizike za osobne podatke, proveli organizacijske i tehničke zaštitne mjere. Osim izrađene GDPR dokumentacije angažirali smo vanjskog neovisnog konzultanta koji je kroz Izvještaj ocijenio razinu usklađenosti s Uredbom.

Svjesni smo da je provedba zaštite osobnih podataka (GDPR) kontinuiran proces koji zahtjeva stalnu brigu o sustavu. Naša namjera je svesti rizik povezan s neovlaštenom i nezakonitom obradom podataka na minimum. Ono uključuje mogućnost slučajnog gubitka osobnih podataka, uništenja, oštećenja podataka. Obrada podatka će biti zakonita, poštena i transparentna obrađivana te isključivo za svrhe zbog kojih je i prikupljana. Želimo biti poslovna organizacija kojoj se vjeruje. Dokument koji potvrđuje našu namjeru je Politika zaštite osobnih podataka koja je javno objavljena.

2.1.7. **Analiza osobnih podataka i njihova obrada**

Komunalno Ozalj d.o.o. je napravio analizu osobnih podataka kako bi se znalo što od osobnih podataka prikuplja i obrađuje. Analiza je napravljena prema svim zainteresiranim stranama čiji interes postoji vezan za zaštitu osobnih podataka. To su naši zaposlenici, korisnici usluge, dobavljači i partneri. GDPR propisuje zaštitu osobnih podataka samo za fizičke osobe. Osobni podatak fizičkih osoba je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (ispitanik osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin

fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet. Podaci koji se smatraju osobnima i ulaze u domenu GDPR-a ne moraju biti istiniti i točni. Oni svejedno podliježu GDPR-u.

Od osobnih podataka zaposlenika najviše prikupljamo podatke koji su potrebni kako bi se proveo zakonski zahtjev obrade, kao npr. kod obračuna plaće. To su podaci vezani za ime i prezime zaposlenika, OIB, adresu stanovanja, datum rođenja i slični podaci koji otkrivaju njegov identitet. Za sve osobne podatke koji nemaju zakonsku osnovu odnosno koji se prikupljaju van pravnog legitimiteta tražena je privola. Privole je moguće pronaći u zapisima GDPR dokumentacije.

Prema analizi osobnih podataka koje prikupljamo odredili smo svrhu njihove obrade. Obradom podataka se podrazumijeva svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima.

Komunalno Ozalj d.o.o. vodi evidenciju obrade podataka. Evidencija se treba dati na uvid nadležnom tijelu ako je potrebito. Evidencije podataka se drže na jednom mjestu, u zaštićenim bazama podataka. Podaci se koristite samo u onu svrhu koja je naznačena u privoli. Prilikom prijenosa podataka u treće zemlje, o tome se obavještavaju ispitanici koje upoznajemo s detaljima primatelja i mjerama sigurnosti koje smo osigurali. Kod prikupljanja i obrade podataka uvijek se vežemo za vremenski period tijekom kojeg planiramo zadržati osobne podatke.

Analizu i obradu osobnih podataka moguće je pronaći u dokumentu Evidencija aktivnosti obrade osobnih podataka.

Zadržavanje osobnih podataka

Osobni podaci mogu se zadržavati samo onoliko koliko je potrebno da se ostvari svrha Obrade. To znači da Osobni podaci moraju biti obrisani (ili anonimizirani) onda kada više nisu potrebni Društvu, odnosno kada je vrijeme Zadržavanja određeno primjenjivim propisima isteklo ili, ako je primjenjivo, kada je Privola Ispitanika povučena.

Ponekad, međutim, postoje pravni ili regulatorni zahtjevi da Osobni podaci budu zadržani za određeno razdoblje. Takvi razlozi mogu biti propisani u različitim propisima, uključujući one primjenjive u sferi:

- trgovačkog prava
- poreznog prava
- radnog prava ili bilo kojem drugom segmenta poslovanja Društva.

Razdoblje čuvanja Osobnih podataka mora se razmatrati u kontekstu svake pojedine Obrade:

- neovisno o bilo kojem pravnom ili regulatornom uvjetu navesti razdoblje Zadržavanja relevantnih Osobnih podataka za obradu;
- Koliko dugo će Komunalno Ozalj trebati zadržavati relevantne Osobne podatke za predloženu aktivnost obrade; i
- neovisno je li trajanje predloženog razdoblja Zadržavanja potrebno za svrhe koje su relevantne aktivnosti obrade.

U svakom slučaju, Osobni podaci će biti obrisani ili anonimizirani, ako se ne primjenjuje barem jedno od sljedećeg:

1. Ispitanik je dao Privolu za obradu njegovih ili njezinih Osobnih podatka u jednu ili više posebnih svrha;

2. Obrada je nužna za izvršavanje ugovora u kojem je Ispitanik ugovorna strana ili kako bi se poduzele radnje na zahtjev Ispitanika prije sklapanja ugovora; (uobičajeno, Osobni Podaci će biti uništeni ne samo nakon prestanka ugovora, nego i kako druge odredbe zakona mogu zahtijevati za određena razdoblja zadržavanja);
3. Obrada je nužna radi poštovanja pravnih obveza Društva;
4. Obrada je nužna kako bi se zaštitili ključni interesi Ispitanika ili druge fizičke osobe;
5. Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti Društva;
6. Obrada je nužna za potrebe legitimnih interesa Društva ili treće osobe, osim kada su od tih interesa jači interesi ili temeljna prava i slobode Ispitanika koji zahtijevaju zaštitu Osobnih podataka, osobito ako je ispitanik dijete; i/ili
7. ne postoji primjenjiva obveza Zadržavanja.

Svaki zaposlenik mora obavijestiti relevantnu osobu zaduženu za Osobne podatke, ili Službenika o predloženom razdoblju zadržavanja određenih Osobnih podataka, koje se razdoblje potom evidentira u Evidencijama obrade podataka koje vodi Komunalno Ozalj. Takvo razdoblje biti će izračunato uzimajući u obzir: (i) primjenjive Propise; (ii) svrhu obrade Osobnih podataka; te (iii) legitimne interese Društva.

Osobni podaci koje obradi Komunalno Ozalj uvijek se obrađuju u skladu s načelima iz Opće uredbe.

Osobni podaci moraju biti uništeni odgovorno i sistematično.

Radi izbjegavanja sumnje, nikakvi Osobni podaci koji bi mogli biti relevantni u bilo kojem postojećem ili očekivanom sudskom postupku, rješavanju spora ili regulatornom istraživanju ne smiju biti uništeni u bilo kojim okolnostima bez prethodne pisane suglasnosti Službenika.

Ako postoji bilo kakva sumnja oko relevantnosti bilo kojeg Osobnog podatka u vezi s postojećim ili očekivanim sudskim postupkom, rješavanjem spora ili regulatornim istraživanjem, Službenik mora biti konzultiran prije poduzimanja bilo koje radnje.

2.1.8. **Procjena rizika zaštite osobnih podataka**

Svrha procjene rizika za zaštitu osobnih podataka je identificirati rizik koji je povezan s zaštitom osobnih podataka kako ne bi bila narušena prava našim zaposlenicima, kupcima i korisnicima usluge te dobavljačima (partnerima). U Komunalno Ozalj d.o.o. smo svjesni da rizik povezan s osobnim podacima nije moguće izbjeći, međutim naša temeljna zadaća je prevenirati rizik kako bi se smanjio na prihvatljivu razinu. Glavna metodologija kojom se procjenjuju rizici za osobne podatke je izračun ukupne izloženosti riziku koja predstavlja ponderiranu vrijednost vjerojatnosti nastanka rizika i procjene učinka rizika na zaštitu osobnih podataka (VNR x PUR). Vjerojatnost nastanka rizika označavamo oznakom VNR, a procjenu učinka rizika oznakom PUR. Detaljan opis načina procjene rizika se nalazi u dokumentu RU Upravljanje rizicima osobnih podataka.

Vjerojatnost	Ocjena	Opis
Visoka	3	Očekuje se da će se ovaj događaj javiti u većini slučajeva
Srednja	2	Događaj se ponekad može javit
Niska	1	Nastanak događaja nije vjerojatan

Učinak	Ocjena	Opis
Velik	3	Učinak rizika na zaštitu osobnih podataka i plaćanje kazne

		je velik.
Umjeren	2	Učinak rizika na zaštitu osobnih podataka je umjeren. Kazna koja bi se platila je umjerena.
Malen	1	Učinak rizika na zaštitu osobnih podataka je malen. Nema kazne za Organizaciju.

2.1.9. **Tehničke i organizacijske mjere sigurnosti**

Unutar Komunalnog Ozalj d.o.o. prema procijenjenim rizicima za osobne podatke uspostavili smo čitav niz tehničkih i organizacijskih mjera zaštite osobnih podataka. Prepoznali smo najmanje 9 mjera zaštite osobnih podataka prema izloženosti rizika. Izloženost riziku može biti mala, srednja i velika. Mali rizik odgovara rezultatu umnošku VNR*PUR koji je 1 i 2, srednji rizik rezultatu umnoška koji je 3 i 4,a veliki rizik rezultatu umnoška koji je 6 i 9.

9 VELIK RIZIK	Potrebno je odrediti ozbiljne tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost podataka riziku je iznimna. Najveći mogući utjecaj na poslovanje.
6 VELIK RIZIK	Potrebno je odrediti ozbiljne tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost podataka riziku je velika. Velik utjecaj na poslovanje.
4 SREDNJI RIZIK	Potrebno je odrediti srednje tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost riziku je srednja. Srednji utjecaj na poslovanje.
3 SREDNJI RIZIK	Potrebno je odrediti srednje tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost riziku je srednja. Srednji utjecaj na poslovanje.
2 MALI RIZIK	Potrebno je odrediti male tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost riziku je mala. Mali utjecaj na poslovanje.
1 MALI RIZIK	Potrebno je odrediti male tehničke i organizacijske mjere zaštite osobnih podataka. Ukupna izloženost riziku je mala. Mali utjecaj na poslovanje.

Tehničke i organizacijske mjere zaštite (TOM) vezane za smanjivanje rizika za osobne podatke su sljedeće:

- TOM 1. Edukacija zaposlenika
- TOM 2. Interni audit
- TOM 3. Zaštita uredskih dokumenata
- TOM 4. Zaštita računala
- TOM 5. Laptopi i mobilni telefoni

- TOM 6. Uništavanje podataka
- TOM 7. Antivirusna politika
- TOM 8. Ponašanje zaposlenika
- TOM 9. Ugovor s vanjskim stranama

Svaka od mjera je propisana, odobrena te implementirana u sustav upravljanja zaštitom osobnih podataka prema GDPR uredbi. Službenik za zaštitu osobnih podataka je upoznao sve zaposlenika s mjerama zaštite osobnih podataka. Mjere je moguće pronaći u istoimenom folderu GDPR dokumentacije koji se zove Tehničko organizacijske mjere zaštite (TOM-ovi).

2.1.10. **GDPR dokumentacija**

GDPR dokumentacija je naziv za zbirku (set) dokumenta koji potvrđuje uspostavljen sustav zaštite osobnih podataka. Svaki od dokumenta potvrđuje namjeru da Organizacija uspostavi, uskladi i upravlja zaštitom osobnih podataka. Dokumentacijom se upravlja jer ima svoj datum i izdanje. GDPR dokumentacija se mora kontinuirano unaprjeđivati. Dokument opisuje kako se GDPR dokumentacijom upravlja je RU Upravljanje GDPR dokumentacijom. Vrste dokumenata koje čine GDPR dokumentaciju su:

- Pravilnik zaštite osobnih podataka
- Zapisi
- Tehničko organizacijske mjere zaštite osobnih podataka (TOM-ovi)
- Radne upute
- Evidencije
- Privole
- Procedure

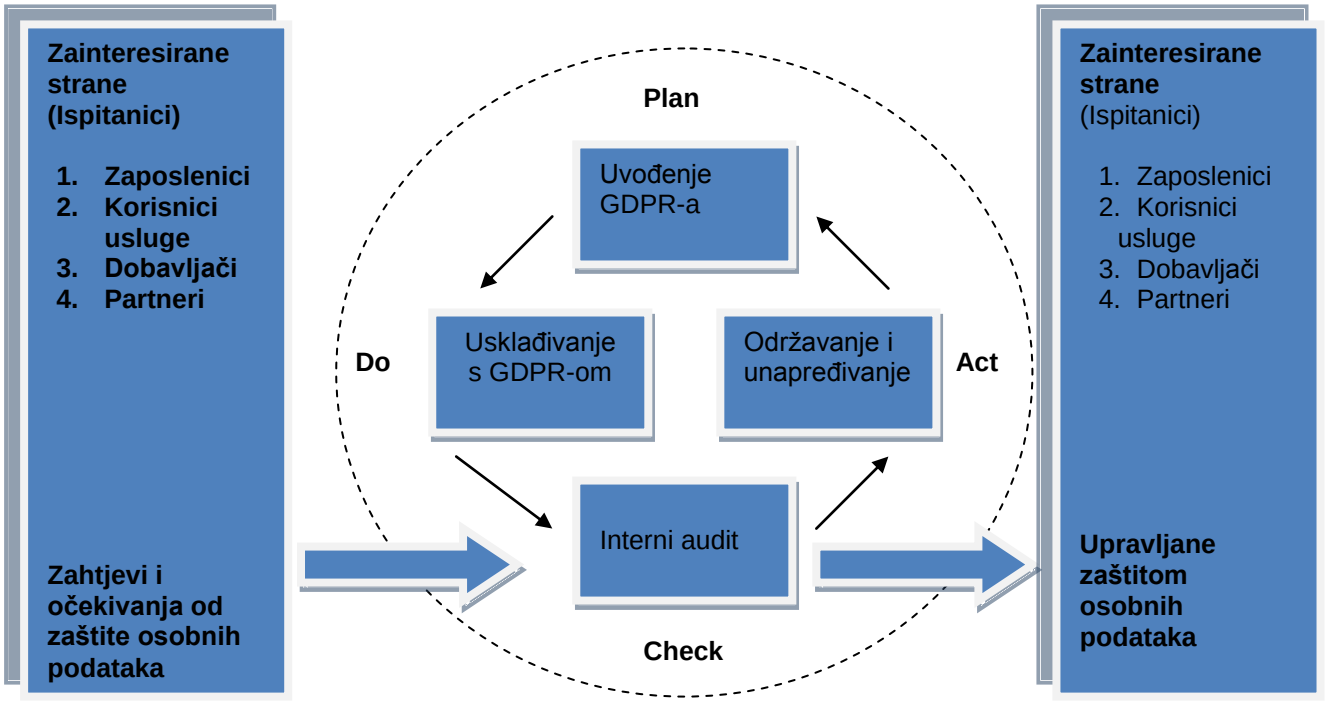
2.1.11. **Audit**

Komunalno Ozalj d.o.o. je uveo i uskladio GDPR sa svojim poslovanjem. Kako bi se postignula što veća efikasnost zaštite osobnih podataka potrebno je povremeno napraviti ocjenu (audit) upravljanja zaštitom osobnih podataka. To će se raditi jedanput godišnje.

Razlog tome leži u potrebi ažuriranja dokumentacije, izradi nove dokumentacije, ali i zbog praćenja svih zakonskih promjena koje mogu utjecati na uspostavljen sustav zaštite osobnih podataka. Učestalost provedbe ocjene sustava zaštite osobnih podataka procijenjen je na osnovi količine i osjetljivosti osobnih podataka koji se obrađuju. Komunalno Ozalj d.o.o. je odredio najmanje jedanput godišnje provesti interni audit. U to ime se mogu angažirati i konzultanti koji će nepristrano i objektivno ocijeniti sustav upravljanja zaštitom osobnih podataka što će povećati kredibilitet uspostavljenog GDPR-a.

Osim internih audita koji će se provoditi samostalno ili s konzultantom, Komunalno Ozalj d.o.o. može povremeno u svrhu zaštite osobnih podataka ocjenjivati svoje dobavljače ili vanjske partnere. Takav audit se zove audit druge strane, a razlozi su uglavnom slijedeći: provjera, selektiranje i potvrđivanje vlastitih dobavljača, poboljšanje vlastitog sustava upravljanja zaštite osobnih podataka, povećanje uzajamne svijesti o važnosti sustava osobnih podataka. Svjesni smo kako Komunalno Ozalj d.o.o. razmjenjuje osobne podatke s drugim voditeljima obrade te kako njihovi propusti u zaštiti osobnih podataka mogu značiti i naše propuste. U to ime, provjerili smo kakve mjere zaštite imaju naši dobavljači odnosno vanjski partneri. Pregledavani su ugovori gdje se razmatralo na koji način je postignuta zaštita osobnih podataka, da li postoje članci koji se vežu za povjerljivost osobnih

podataka. S onim dobavljačima, vanjskim stranama dodatno su potpisani Ugovori za zaštitu osobnih podataka.



Slika 3. : PDCA krug u GDPR-u

2.1.12. **Privole**

Komunalno Ozalj d.o.o. je tražio od svih zainteresiranih strana (ispitanika) dobrovoljno, informirano, nedvosmisleno izražavanje želje ispitanika vezano za pristanak na obradu njegovih osobnih podataka. Time je Komunalno Ozalj d.o.o. omogućio pravo izbora korisnicima usluge, zaposlenicima, dobavljačima i partnerima vezano za obradu njihovih podataka. Privolom smo omogućili da nam odobre obradu osobnih podataka ali smo ih osvijestili da u svakom trenutku mogu povući svoju privolu i to bez prijetnji nekim drugim ishodom koji bi bio loš za njih same.

Za svaku novu svrhu obrade ishoditi ćemo novu zasebnu privolu kako bi izbjegli mogućnost da budemo dvosmisleni. Cilj privole je steći povjerenje bez obzira da li je riječ o našim korisnicima usluge ili zaposlenicima te dobavljačima (partnerima). Privola će sadržavati podatke preko kojih će se ispitanik moći informirati o voditelju obrade, svrsi obrade, vrsti podataka koji se prikupljaju, namjeri postupanja s podacima.

Kako bi u svakom trenutku mogli dokazati zakonitost rada (obrade podataka), privole ćemo čuvati. Privole ćemo čuvati i nakon što završi aktivnost obrade osobnih podataka. Valjanost privole je vremenski neograničena. Odgovornost za prikupljanje privola pripada Službeniku za zaštitu osobnih podataka. Privole je moguće pronaći u istoimenom folderu GDPR dokumentacije.

2.1.13. *Prava postupanja i procedure*

Ako zaposlenici doznaju za potencijalnu Povredu podataka u Komunalnom Ozalj d.o.o, obvezni su odmah obavijestiti osobu zaduženu za poslove zaštite podataka ili Službenika.

Službenik će odmah poduzeti potrebne korake i obavijestiti upravu Društva i druge osobe uključene u stvari obrade Osobnih podataka.

Do Povrede podataka može doći zbog mnogih razloga. Na primjer, Povreda podataka može uključivati:

- namjerne pokušaje od strane zaposlenika ili trećih osoba da ostvare neovlašten pristup Osobnih podacima;
- neovlašteno otkrivanje Osobnih podataka Osoblju Društva ili trećim osobama;
- gubitak ili krađu podataka ili opreme na kojoj su Osobni podaci pohranjeni (npr. gubitak prijenosnog računala koje sadrži takve podatke);
- prepisku koja uključuje Osobne podatke, a koja je poslana pogrešnom primatelju (npr. netko pošalje email koji sadrži takve podatke pogrešnoj osobi); i/ili
- slabosti u internoj kontroli koje mogu dovesti do neovlaštenog otkrivanja, zlouporabe, gubitka, izmjene ili uništenja Osobnih podataka.

Službenik je obvezan doznati više od situaciji te odmah angažirati sve potrebne stručnjake za takve situacije, npr. vanjske specijaliste, kako bi se razjasnilo:

- koja je priroda i opseg Osobnih podataka;
- koja je priroda i broj Ispitanika;
- koje su posebne kategorije osobnih podataka i/ili osobni podaci koji se odnose na kaznene osude i kažnjiva djela;
- koji su informatički sustavi i procesi zahvaćeni potencijalnom Povredom podataka te sve ostalo potrebno za adekvatno postupanje.

Ako Službenik smatra da je vjerojatnije da je došlo do Povrede podataka nego da nije, Službenik će odmah obavijestiti upravu i relevantnog Vlasnika Imovine.

Uklanjanje povrede

Ne postoji jedan standardan način za reagiranje na Povredu podataka. Na svaku Povredu podataka potrebno je reagirati na jedinstven način ovisno o okolnostima konkretnog slučaja, te izvršiti procjenu rizika koje ona uključuje. Potom je takvu procjenu rizika potrebno koristiti kao osnovu za donošenje odluke o tome koju je radnju potrebno izvršiti u konkretnim okolnostima, te je potrebno utvrditi koje odredbe zakona o zaštiti podataka su primjenjive, npr. obveza obavješćivanja nadležnog nadzornog tijela – u Hrvatskoj, Agencije za zaštitu osobnih podataka ("*AZOP*").

Kako bi se upravljalo takvom kriznom situacijom, potrebno je osnovati vješt i ovlašten Tim za odgovaranje na povredu podataka ("*Tim*"), koji se u pravilu sastoji od sljedećih članova:

- član uprave;
- Službenik;

Tim se može proširiti, ako okolnosti to zahtijevaju.

Tim je odgovoran za:

- koordiniranje cjelokupnog procesa, uključujući sve analize i protumjere;

- organiziranje redovitih sastanaka – ako je to potrebno – kako bi se osigurala razmjena informacija o slučaju; te
- upravljanje komunikacijom sa svim zainteresiranim osobama, ovisno o okolnostima konkretnog slučaja.

Tim će odmah poduzeti radnje kako bi osigurao da će sljedeći zadaci biti izvršeni

- procjenjivanje i razumijevanje uzroka Povrede podataka;
- utvrđivanje koje su osobe i koji su Osobni podaci pogođeni Povredom podataka;
- utvrđivanje vjerojatnih posljedica za pogođene Osobne podatke;
- utvrđivanje postoji li neposredna ili buduća opasnost po ostale sustave ili procese; i
- utvrđivanje kratkoročnih tehničkih i organizacijskih mjera koje je potrebno provesti kako bi se osiguralo pogođene Osobne podatke, informatičke sustave i/ili procese.

Sva prepiska, komunikacija i dokumentacija koja se odnosi na slučaj Povrede podataka u načelu treba biti dokumentirana i označena kao "Povjerljivo".

Tim će sastaviti zapisnik s opisom svih poduzetih mjera i analizom utvrđenog stanja.

Dužnost izvještavanja

U slučaju da se otkrije Povreda podataka, Komunalno Ozalj mora izvijestiti AZOP bez nepotrebne odgode, po otkrivanju incidenta koji je uzrokovao ili može uzrokovati Povredu podataka. Jednako tako, Izvršitelj obrade za Komunalno Ozalj d.o.o. mora obavijestiti Komunalno Ozalj d.o.o. bez nepotrebnog odgađanja nakon što postane svjestan da je nastala Povreda podataka.

Međutim, unatoč Povredi podataka, ni jedno izvještavanje AZOP nije potrebno ako nije vjerojatno da će povreda "prouzročiti rizik za prava i slobode pojedinaca". Kako bi procijenila rizik, Komunalno Ozalj mora uzeti u obzir kombinaciju ozbiljnosti potencijalnog utjecaja na prava i slobode pojedinaca i mogućnost da se ti utjecaji dogode.

Komunalno Ozalj bi trebala pažljivo obaviti svoju zadaću izvješćivanja.

U izvješćivanju se mora (barem):

- opisati priroda Povrede podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj zahvaćenih procesa koji sadrže Osobne podatke;
- navesti ime i kontaktne podatke Službenika ili druge kontaktne točke od koje se može dobiti više informacija;
- opisati vjerojatne posljedice Povrede podataka;
- opisati mjere koje je Komunalno Ozalj poduzelo ili predložilo poduzeti za rješavanje problema Povrede podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Izvješće AZOP-u, sukladno odredbama članka 33. Opće uredbe mora biti učinjeno "bez nepotrebnog odgađanja" i ako je izvedivo, najkasnije 72 sata nakon saznanja da se dogodila Povreda podataka. Ako izvješćivanje AZOP-u nije napravljeno unutar 72 sata, izvješćivanje mora sadržavati razloge kašnjenja.

U nekim slučajevima, bit će relativno jasno od početka da se dogodila povreda, dok u drugim, može proteći neko vrijeme da se ustanovi da li je došlo do kompromitiranja (Povrede) Osobnih podataka.

Dužnost izvještavanja pogođenih osoba (Ispitanika)

Tamo gdje je vjerojatno da će povreda podataka rezultirati "visokim rizikom" za prava i slobode pojedinaca, Voditelj obrade mora objasniti povredu podataka Ispitanicima bez nepotrebnog odgađanja.

Obavješćivanje ispitanika nije obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

- Komunalno Ozalj d.o.o. je poduzeo odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na Osobne podatke pogođene Povredom podataka, posebno one mjere koje Osobne podatke čine nerazumljivima bilo kojoj trećoj osobi koja nema ovlaštenje za pristup tim Osobnim podacima (kao što je enkripcija);
- Komunalno Ozalj d.o.o. je poduzeo naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode Ispitanika;
- time bi se zahtijevao nerazmjeran napor u svrhu obavješćivanja pojedinog Ispitanika. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se Ispitanici obavješćuju na jednako djelotvoran način.

Obavijest Ispitanicima, sukladno odredbama članka 34. Opće uredbe mora biti sačinjena bez nepotrebnog odgađanja, što u ovom slučaju znači "čim je to razumno moguće". Na primjer, potreba da se umanji neposredni rizik od štete iziskivala bi brzu komunikaciju s Ispitanicima dok potreba implementacije odgovarajućih mjera protiv neprekinute ili slične Povrede podataka može opravdavati više vremena za komunikaciju.

Dužnost izvještavanja Izvršitelja obrade

Dužnost Izvršitelja obrade da izvijesti Voditelja obrade o svakoj Povredi podataka uvedena je odredbama članka 33. Opće uredbe. Prema tome, tamo gdje Komunalno Ozalj djeluje kao Izvršitelj obrade Osobnih podataka, adekvatne tehničke i organizacijske mjere trebaju biti implementirane kako bi bile u skladu s uvedenom dužnosti. Jednako, Izvršitelji obrade koji djeluju u ime Društva imaju dužnost izvještavanja prema Društvu. Odgovornosti i dužnosti između Izvršitelja obrade i voditelja obrade u slučaju Povrede podataka trebaju biti predviđene ugovorom o obradi osobnih podataka između Voditelja obrade i Izvršitelja obrade.

Ne postoje iznimke. Izvršitelj obrade Osobnih podataka mora izvijestiti Voditelja obrade o bilo kojoj Povredi podataka, neovisno hoće li Povreda podataka vjerojatno predstavljati rizik za prava i slobode pojedinca.

Kako i gdje Izvršitelj obrade treba izvijestiti Voditelja obrade?

Izvješće voditelja obrade Izvršitelju obrade mora imati isti minimalni sadržaj kao i izvješće Voditelja obrade.

Izviješće mora biti napravljeno bez nepotrebnog odgađanja. Smatra se da je voditelj obrade postao "svjestan" Povrede podataka onda kada je Izvršitelj obrade postao svjestan. Prema tome izvješćivanje se treba napraviti odmah, s daljnjim informacijama danim u fazama kako postaju dostupne.

Saniranje Povrede podataka

Nakon što se tekuća situacija vezana uz Povredu podataka stabilizira, a Osobni podaci više ne budu u opasnosti, Tim je obvezan izvršiti sljedeće radnje:
a) provesti analizu ključnog uzroka Povrede podataka;
b) pustiti pogođene informatičke sustave u njihov uobičajen rad;

c) odabrati način primanja upita (npr. email adresa); i
d) pripremiti plan komuniciranja s relevantnim internim i vanjskim zainteresiranim osobama i relevantne komunikacijske kanale (npr. uključujući internetske stranice i društvene mreže), ako je to potrebno.

Komunikacija

Tim je obvezan osigurati dostupnost odgovarajućih komunikacijskih alata. Naročito će osigurati da:

- komunikacija s medijima, Ispitanicima i/ili bilo kojom trećom osobom bude valjano odobrena od strane AZOP-a prije nego bude priopćena primateljima, u slučajevima kada je takvo odobrenje AZOP-a potrebno ili propisano;
- preliminarne informacije i formalna komunikacija s AZOP-om u roku od 72 sata nakon Povrede podataka za koju postoji obveza obavještavanja, budu odobrene prije njihovog priopćavanja;
- se podnese konačni izvještaj AZOP-u nakon što Povreda podataka bude u potpunosti istražena;
- interna komunikacija radnicima bude učinjena prije vanjske komunikacije, ako je to moguće;
- bude poslana obavijest tijelu nadležnom za provedbu zakona, po potrebi.

Popratne radnje nakon Povrede

Nakon što slučaj Povrede podataka bude riješen, Tim je obvezan provesti daljnje mjere u svrhu sprječavanja budućih Slučajeva povreda sigurnosti i Povreda podataka. Naročito je dužan osigurati:

- održavanje sastanka Tima sa svrhom utvrđivanja onoga što je naučeno iz iskustva s navedenim slučajem;
- izradu završnog internog izvješća;
- analizu pogođenih mjera zaštite, kontrole, pravilnika i tehničkih i organizacijskih mjera;
- izradu plana mjera, po potrebi;
- pokretanje naknadnih projekata, po potrebi; i
- održavanje dodatne obuke za radnika, po potrebi**.**

Komunalno Ozalj d.o.o. je kroz Uredbu prepoznao procedure na koje se oslanja po pitanju zaštite osobnih podataka. Procedure su vezane za procese obrade podataka. Komunalno Ozalj d.o.o. ih je potpuno integrirao u svoje poslovanje te kao takve postaju način na koji će organizacija ostvarivati prava po pitanju zaštite osobnih podataka ispitanika. Procedure je moguće pronaći u istoimenom folderu GDPR dokumentacije.

Identificirane procedure su sljedeće:

- Procedura Izvještavanja u svezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade
- Procedura Pravo ispitanika na brisanje podataka
- Procedura Pravo ispitanika na ispravak podataka
- Procedura Pravo ispitanika na zahtjev za zaštitu osobnih podataka
- Procedura Pravo na izvještavanje nadzornog tijela
- Procedura Pravo na obavještavanje ispitanika o povredi osobnih podataka
- Procedura Pravo na prenosivost osobnih podataka
- Procedura Pravo na prigovor

- Procedura Pravo na ograničavanje obrade
- Procedura Pravo na pristup osobnim podacima