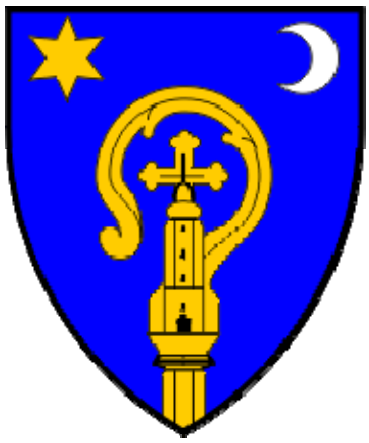

S T R A T E G I J A
zaštite osobnih podataka Grada Dugog Sela

U Dugom Selu, 10. travnja 2019. god.

Sadržaj

1. Uvod

Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo u smislu članka 8. stavka 1. Povelje Europske unije o temeljnim pravima te članka 16. stavka 1. Ugovora o funkcioniranju Europske unije. Također, zaštita osobnih podataka uređena je u okviru osobnih i političkih prava i sloboda odredbom članka 37. Ustava Republike Hrvatske ("Narodne novine", broj 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10 i 05/14) prema kojoj se svakome jamči sigurnost i tajnost osobnih podataka, a osobni se podaci mogu, bez privole ispitanika, prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.

Stupanjem na snagu Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka; u daljnjem tekstu: GDPR), percepcija zaštite osobnih podataka dobila je sasvim drugu dimenziju kako stručne tako i sveukupne šire javnosti s obzirom na doseg primjene. S obzirom na prilično apstraktan tekst GDPR-a te brojne neodređene formulacije koje se odnose na prava ispitanika i obveze voditelja obrade osobnih podataka, jasne i nedvosmislene odgovore na brojna pitanja tek će dati praksa koja je, u vrijeme nastanaka ove Strategije tek u svojoj predparadigmatskoj fazi. Uzroke za takvu eventualnu neodređenost nalazimo u okviru okolnosti da je GDPR propis koji je potrebno primijeniti i implementirati u pravne sustave svih 28 država članica Europske unije.

Nadalje, jedna od značajki GDPR-a svakako se odnosi na univerzalnost primjene za sve pravne i fizičke osobe koje u okviru svojih djelatnosti, bez obzira je li riječ o javnim tijelima, pravnim ili fizičkim osobama registriranim za obavljanje različitih djelatnosti ili drugim organizacijama u najširem smislu, obrađuju osobne podatke. Osnovne pojmove i definicije koje se odnose na obradu osobnih podataka u kontekstu GDPR-a navest ćemo *infra* u tekstu. Uvažavajući tako navedenu univerzalnost primjene na izrazito širok spektar različitih obveznika, lako se može izvesti zaključak kako je usklađivanje i prilagođavanje poslovnih i inih procesa koji obuhvaćaju obradu osobnih podataka potrebno prilagoditi specifičnim djelatnostima ili grupama djelatnosti različitih obveznika. Primjera radi, ne može se očekivati da će za jedinice lokalne ili područne (regionalne) samouprave u okviru obavljanja svojih javnih zadaća i ovlasti biti moguće urediti politike i strategije zaštitu osobnih podatka na isti način kao i za trgovačka društva čija se osnovna djelatnost odnosi ne sve raširenju i, obzirom na rast digitalnog društva, sve prisutniju djelatnost digitalnog oglašavanja. U istom smislu valja napomenuti kako pravo na zaštitu osobnih podataka nije apsolutno pravo već ga se mora razmatrati u vezi s njegovom funkcijom u društvu te ga je potrebno uskladiti i ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti.

Slijedom navedenog, ovom Strategijom je potrebno obuhvatiti i analizirati sve osobne podatke koje Grad Dugo Selo (u daljnjem tekstu: Grad) u okviru svojih na zakonu utemeljenih prava i ovlasti prikuplja i obrađuje, utvrditi zakonsku osnovu prikupljanja takvih podataka prema upravnim i drugim područjima svoje djelatnosti, definirati odgovarajuće organizacijske i tehničke mjere zaštite osobnih podataka te jasno poznavati sva prava i obveze koje je potrebno poštivati kako bi se učinkovito provelo usklađivanje s GDPR-om te izbjeglo bilo kakve potencijalno negativne i štetne posljedice kako za ispitanike, tako i za Grad. Također, postoje odredbe GDPR-a koje se odnose na prenosivost podataka, međunarodnu suradnju ili pojedine mjere zaštite za koje smatramo kako ih, uvažavajući specifičnosti osnova za prikupljanje podataka od strane Grada, u ovom trenutku nije potrebno detaljnije analizirati.

Prije nastavka analize prava, obveza i radnji koje je potrebno poduzeti kako bi Grad u smislu zaštite osobnih podataka postigao usklađenost s GDPR-om, u nastavku citiramo odredbu članka (4) Uvodne izjave GDPR-a koja glasi:

„Obrada osobnih podataka trebala bi biti osmišljena tako da bude u službi čovječanstva. Pravo na zaštitu osobnih podataka nije apsolutno pravo; mora ga se razmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti.“

2. O Gradu Dugom Selu

Zakonom o području županija, gradova i općina u Republici Hrvatskoj (''Narodne novine'', broj 86/06, 125/06, 16/07, 95/08, 46/10, 145/10, 37/13, 44/13, 45/13 i 110/15) utvrđeno je da je Dugo Selo grad u sastavu Zagrebačke županije koji obuhvaća ukupno 11 naselja, dok je odredbom članka 5. Zakona o lokalnoj i područnoj (regionalnoj) samoupravi (''Narodne novine'', broj 33/01, 60/01 – vjerodostojno tumačenje, 129/05, 109/07, 125/08, 36/09, 150/11, 144/12 i 19/13 – pročišćeni tekst, 137/15 - ispravak i 123/17; u daljnjem tekstu: ZLP(R)S) određeno kako je grad jedinica lokalne samouprave koja predstavlja urbanu, povijesnu, prirodnu, gospodarsku i društvenu cjelinu, a u sastav grada kao jedinice lokalne samouprave mogu biti uključena i prigradska naselja koja s gradskim naseljem čine gospodarsku i društvenu cjelinu te su s njim povezana dnevnim migracijskim kretanjima i svakodnevnim potrebama stanovništva od lokalnog značenja.

Odredbom članka 19. ZLP(R)S-a propisani su poslovi koji se stavljaju u nadležnost gradova i općina pa isti članak navodimo u nastavku u cijelosti:

„Općine i gradovi u svom samoupravnom djelokrugu obavljaju poslove lokalnog značaja kojima se neposredno ostvaruju potrebe građana, a koji nisu Ustavom ili zakonom dodijeljeni državnim tijelima i to osobito poslove koji se odnose na:

- *uređenje naselja i stanovanje,*
- *prostorno i urbanističko planiranje,*
- *komunalno gospodarstvo,*
- *brigu o djeci,*
- *socijalnu skrb,*
- *primarnu zdravstvenu zaštitu,*
- *odgoj i osnovno obrazovanje,*
- *kulturu, tjelesnu kulturu i šport,*
- *zaštitu potrošača,*
- *zaštitu i unapređenje prirodnog okoliša,*
- *protupožarnu i civilnu zaštitu,*
- *promet na svom području*
- *te ostale poslove sukladno posebnim zakonima.*

Posebnim zakonima kojima se uređuju pojedine djelatnosti iz stavka 1. ovoga članka odredit će se poslovi čije su obavljanje općine i gradovi dužni organizirati te poslovi koje mogu obavljati.“

U skladu s ovlastima na temelju gore citiranog Zakona kojim se, između ostaloga, uređuju jedinice lokalne samouprave, njihov djelokrug i ustrojstvo, način rada njihovih tijela, nadzor nad njihovim aktima i radom te druga pitanja od značenja za njihov rad, Grad donosi

podzakonske akte kojima se ista pitanja detaljnije razrađuju. Tako je Gradsko vijeće Grada Dugog Sela - na 12. sjednici, održanoj 6. srpnja 2010. godine, donijelo Odluku o ustrojstvu i djelokrugu upravnih tijela Grada Dugog Sela (Službeni Glasnik Grada Dugog Sela, broj 7/10; u daljnjem tekstu: Odluka) kojom se uređuje ustrojstvo upravnih tijela Grada, njihov djelokrug u obavljanju samoupravnih poslova, upravljanje upravnim tijelima, odgovornost za zakonito i pravilno obavljanje poslova i sredstva za njihobo obavljanje.

Za obavljanje poslova iz samoupravnog djelokruga ustrojena se sljedeća upravna tijela:
1. Upravni odjel za poslove Gradskog vijeća i Gradonačelnika,
2. Upravni odjel za gospodarstvo i financije,
3. Upravni odjel za prostorno uređenje, zaštitu okoliša, komunalno i stambeno gospodarstvo,
4. Upravni odjel za društvene djelatnosti.

3. Normativni okvir

Budući da je Republika Hrvatska članica Europske unije, normativni okvir više nije moguće svesti na nacionalno zakonodavstvo i podzakonske akte kojima se uređuje određeno područje, već je isti nužno analizirati, tumačiti i primjenjivati kroz međunarodnu komponentu. Tako, u smislu ove Strategije, normativni okvir u užem smislu čini niz propisa kojima se izravno uređuje zaštita osobnih podataka, a temeljni propis je upravo naprijed citirani GDPR. Važno je naglasiti da je GDPR u cijelosti obvezujući te da se primjenjuje izravno u svim državama članicama EU, dok su na temelju istog države članice bile u obvezi donijeti zakone kojima pobliže razrađuju i uređuju prava i obveze kako nadzornih tijela tako i ispitanika, odnosno voditelja i izvršitelja obrade. Republika Hrvatska je stoga donijela Zakon o provedbi opće uredbe o zaštiti podataka ("Narodne novine", broj 42/18; u daljnjem tekstu: Zakon) koji je stupio na snagu 25. svibnja 2018. godine, uz napomenu kako su stupanjem na snagu Zakona prestali važiti Zakon o zaštiti osobnih podataka ("Narodne novine", broj 103/03, 118/06, 41/08, 130/11 i 106/12 – pročišćeni tekst), Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka ("Narodne novine", broj 105/04) i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka ("Narodne novine", broj 139/04).

Iako Zakon više ne propisuje obvezu prijave evidencija Agenciji za zaštitu osobnih podataka (u daljnjem tekstu: AZOP) te se na prvi pogled može lako stvoriti privid kako je riječ o manje obveza za sve organizacije na čije se djelovanje GDPR primjenjuje, pravo stanje stvari je puno kompleksnije te zahtijeva ozbiljan i sistematičan pristup čitavom području zaštite osobnih podataka. U razdoblju od donošenja GDPR-a pa do stupanja na snagu istog s danom 25. svibnja 2018. godine, zaštita podataka dobila je prilično drugačiju dimenziju te, zahvaljujući izrazitom interesu i angažmanu medija te IT industrije, postala jedna od najatraktivnijih tema šire (ne samo stručne) javnosti.

Neodređenost i apstraktnost pojedinih odredbi, kao i univerzalna primjenjivost GDPR-a na gotovo sve javnopravne i privatne entitete koji obrađuju podatke fizičkih osoba, stvaraju poteškoće u jasnom i nedvojbenom definiranju svih obveza za određena tijela koje je potrebno poštovati kako bi se postigla usklađenost s GDPR-om.

a) Međunarodni normativni okvir

Međunarodni normativni okvir u području zaštite podataka u širem smislu čine:

- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) ili GDPR
- Direktiva (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije
- Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji
- The "Article 29 Working Party" – radna skupina ustrojena i osnovana na temelju čl. 29. Direktive 95/46/EC
    - Smjernice o pravu na prenosivost podataka donesene 13. prosinca 2016., zadnje revidirane i donesene 5. travnja 2017.
    - Smjernice za identifikaciju voditelja obrade ili vodećeg nadzornog tijela izvršitelja od 13. prosinca 2016.
    - Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679, od 4. travnja 2017.
    - Smjernice o službenicima za zaštitu podataka donesene 13. prosinca 2016., zadnje revidirane i donesene 5. travnja 2017. i
    - Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679 od 3. listopada 2017.

(Europski odbor za zaštitu podataka (EOZP) trebao bi u skladu s člankom (139) uvodne izjave GDPR-a zamijeniti Radnu skupinu za zaštitu pojedinaca u vezi s obradom osobnih podataka osnovanu Direktivom 95/46/EZ te nastaviti donositi smjernice kako bi se osigurala dosljedna primjena prava o zaštiti podataka diljem EU-a, iz čega se može izvesti zaključak kako postupak i proces izrade normativnog okvira u širem smislu još nije okončan.)

b) Nacionalni normativni okvir

Analizirajući upravna i druga područja u nadležnosti Grada, normativni okvir u smislu ovog dokumenta mogao bi se proširiti na gotovo sve propise u okviru kojih se odlučuje o pravima i obvezama fizičkih osoba. Stoga je pri navođenju normativnog okvira važno držati se temeljnih propisa koji uređuju predmetno područje, ali i, s obzirom na međusobno preklapanje određenih prava i obveza, u ovom smislu navesti osobito propise kojima se uređuje područje prava na pristup informacijama te područje postupanja s arhivskim gradivom.

Nacionalni normativni okvir u širem smislu čine:

- članak 37. Ustava Republike Hrvatske ("Narodne novine", broj 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10 i 05/14)
- Zakon o provedbi Opće uredbe o zaštiti podataka ("Narodne novine", broj 42/18)
- Zakon o zaštiti osobnih podataka ("Narodne novine", broj 103/03, 118/06, 41/08, 130/11 i 106/12) – prestao važiti 25. svibnja 2018.
- Zakon o akreditaciji ("Narodne novine", broj 158/03, 75/09 i 56/13) - zbog EN-ISO/IEC 17065/2012 iz članka 43. GDPR

- Zakon o pravu na pristup informacijama (''Narodne novine'', broj 25/13 i 85/15) i
- Zakon o arhivskom gradivu i arhivima (''Narodne novine'', broj 61/18).

Naprijed je naveden dio normativnog okvira u širem smislu, uz napomenu kako, s obzirom na specifična područja u djelokrugu Grada, držimo izrazito važnim navesti osobito zakone o pravu na pristup informacijama, odnosno o arhivskom gradivu i arhivima.

Također, a zaključno u ovom dijelu, ističemo kako je postojeći normativni okvir nužno promatrati kao polaznu točku u rješavanju svih pitanja vezanih uz zaštitu osobnih podataka, dok će praksa kako AZOP-a tako i EOZP-a, uključujući praksu nadležnih sudova, tek dati neke jasnije odgovore na brojna pitanja koja imaju apstraktan ili neodređen karakter.

c) Načela obrade osobnih podataka

Iako načela u širem smislu predstavljaju pravne norme koje omogućavaju rješavanje pravnih situacija za koje ne postoji jasno, bezuvjetno i precizno pisano pravno pravilo, njihova važnost nije upitna te se u nastavku, obzirom da se njime utvrđuju načela obrade osobnih podataka, navodi u cijelosti članak 5. GDPR-a:

„Članak 5.
Načela obrade osobnih podataka

1. Osobni podaci moraju biti:
(a) zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika („zakonitost, poštenost i transparentnost”);

(b) prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 89. stavkom 1. ne smatra se neusklađenom s prvotnim svrhama („ograničavanje svrhe”);

(c) primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka”);

(d) točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu ili isprave („točnost”);

(e) čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; osobni podaci mogu se pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 89. stavkom 1., što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih ovom Uredbom radi zaštite prava i sloboda ispitanika („ograničenje pohrane”);

(f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („cjelovitost i povjerljivost”).

2. Voditelj obrade odgovoran je za usklađenosti sa stavkom 1. te je mora biti u mogućnosti dokazati („pouzdanost”).“

Iz citiranog članka također proizlazi kako je voditelj obrade odgovoran za usklađenost obrade osobnih podataka iz svoje nadležnosti te kako istu mora biti u mogućnosti dokazati kako ispitanicima tako i nadležnom tijelu.

d) Odnos prema pravu na pristup informacijama

Pravo na pristup informacijama i obveza zaštite osobnih podataka nisu apstraktni pojmovi kojima se bave teoretičari i stručnjaci, već vrlo životna prava i obveze implementirane u gotovo svim sustavima i organizacijama. Međutim, iako bi diskurs o tome je li riječ o kontradiktornim ili komplementarnim područjima ipak trebalo prepustiti pravnim stručnjacima, posljedice koje određena činjenja ili propuštanja mogu uzrokovati su itekako stvarne.

Informacija je svaki podatak koji posjeduje tijelo javne vlasti, neovisno o obliku u kojem je nastala, a pravo na pristup informacijama je pravo svih fizičkih i pravnih osoba na dobivanje informacija koje posjeduju tijela javne vlasti u Republici Hrvatskoj, neovisno o svrsi u koju se informacija želi koristiti.

Ovdje ćemo se samo osvrnuti na odredbu članka 15. stavka 2. točke 4. Zakona o pravu na pristup informacijama ("Narodne novine", broj 25/13 i 85/15) prema kojoj tijela javne vlasti mogu ograničiti pristup informaciji ako je informacija zaštićena zakonom kojim se uređuje područje zaštite osobnih podataka.

Normativni okvir predmetnih područja je prilično apstraktan i neodređen, a očitovanja nadležnih tijela u predmetima gdje dolazi do preklapanja navedenih prava samo potvrđuju takav stav.

U nedostatku čvrstih temelja za izražavanje konkretnih stavova po tom pitanju, možemo zaključiti kako je objava osobnih podataka, u slučaju da za istu postoji odgovarajući pravni temelj, zakonita. Međutim, prilikom objave takvih podataka s ciljem informiranja javnosti, uvijek valja voditi računa da se ne objavljuju oni podaci koji predstavljaju prekomjernu obradu osobnih podataka.

Za sve ostale slučajeve potrebno je u skladu s načelom razmjernosti posebno utvrđivati koje od navedenih prava prevladava u svakom konkretnom slučaju te u tom smislu postupiti prema zahtjevu za pristup informacijama. Preporuka je svakako ne davati službene isprave koje sadrže osobne podatke, a osobito one koje sadrže posebne kategorije osobnih podataka (e.g. platne liste službenika ili rješenja o pravima korisnika u području socijalne skrbi) u svim slučajevima kada podnositelj zahtjeva informaciju može dobiti na temelju drugih podataka ili javno dostupnih izvora.

e) Odnos prema propisima o arhivskom gradivu

Prema odredbama Zakona o arhivskom gradivu i arhivima ("Narodne novine", broj 61/18), grad je tijelo javne vlasti te kao takvo stvara javno arhivsko gradivo. Ovu okolnost valja osobito istaknuti u kontekstu ostvarivanja prava ispitanika u odnosu na odredbe GDPR-a koje propisuju prava i obveze voditelja obrade. Tako je u članku (62) Uvodne izjave GDPR-a navedeno kako obvezu pružanja informacija ipak nije potrebno nametati ako ispitanik već posjeduje tu informaciju, ako je bilježenje ili otkrivanje osobnih podataka izrijekom

propisano zakonom ili ako je pružanje informacije ispitaniku nemoguće ili bi zahtijevalo nerazmjeran napor. Primjer nemogućnosti pružanja informacija ili nerazmjernog napora posebno bi se mogao javiti ako se obrada obavlja u svrhe arhiviranja u javnom interesu, u svrhe znanstvenih ili povijesnih istraživanja ili u statističke svrhe. Slična formulacija nalazi se i u odredbi članka 14. stavka 5. točke (b) GDPR-a koja određuje koje informacije se trebaju pružiti ako osobni podaci nisu dobiveni od ispitanika, odnosno kako se ispitaniku ne pružaju tražene informacije ako je pružanje takvih informacija nemoguće ili bi zahtijevalo nerazmjerne napore, posebno za obrade u svrhe arhiviranja u javnom interesu.

4. Osnovni pojmovi i definicije

Odredbom članka 4. GDPR-a, s obzirom na okolnost da je isti potrebno primijeniti u okviru pravnih sustava svih 28 država članica, utvrđuju se pojmovi i definicije vezane uz područje zaštite osobnih podataka. Ovo osobito ističemo u smislu članka 3. Zakona o provedbi opće uredbe o zaštiti podataka prema kojem pojmovi u smislu Zakona imaju jednako značenje kao pojmovi korišteni u GDPR-u, slijedom čega zaključujemo kako, bez obzira na njihovu gramatičku ili teleološku sličnost s nekim drugim pravnim institutima ili pojmovima, nije poželjno primjenjivati relevantne pojmove i sintagme uređene drugim propisima. Također, uvažavajući organizacijske specifičnosti i djelokrug rada Grada, u nastavku se navode neki temeljni pojmovi GDPR-a nužni za što potpunije i pravilnije usklađenje s istim:

- OSOBNI PODACI - 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 - 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;

- SUSTAV POHRANE - svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;

- PODUZEĆE - 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;

- VODITELJ OBRADE - 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 - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;

- PRIVOLA - 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;

- NADZORNO TIJELO - neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. GDPR-a (nap. a.: u RH je to AZOP).

5. Zakonitost obrade osobnih podataka

U članku 6. stavku 1. GDPR-a propisano je kako je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:
(a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
(b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
(c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade
(d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe
(e) **obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade**
(f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete (ne odnosi se na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća).

Ako je pravni temelj za obradu osobnih podataka pravna obveza voditelja obrade, tada ta pravna osnova mora biti utvrđena u pravu Unije ili pravu države članice kojem voditelj obrade podliježe, a tom pravnom osnovom mora biti određena i svrha obrade.

Budući da je Grad jedinica lokalne samouprave koja, u skladu sa *supra* navedenim normativnim okvirom, **obavlja zadaće od javnog interesa u okviru svojih službenih ovlasti**, odnosno poštujući različite pravne obveze u okviru svog djelovanja, zakonitost obrade velike većine osobnih podataka koje u tom smislu obrađuje nije dvojbena ni upitna. To ne znači kako neke podatke Grad ne može prikupljati na temelju privole (e. g. stipendije) ili ako je obrada nužna za izvršavanje ugovora u kojem je ispitanik stranka, odnosno kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora.

U kontekstu navođenja normativnog okvira i pravne osnove za obradu osobnih podataka, pored odredbi ZLP(R)S-a i drugih propisa koji detaljnije uređuju područja nadležnosti Grada, valja svakako navesti i odredbu članka 47. Zakona o proračunu (''Narodne novine'', broj 87/08, 136/12 i 15/15) prema kojoj su proračunski korisnici i tijela jedinica lokalne i područne (regionalne) samouprave odgovorni za potpunu i pravodobnu naplatu prihoda i primitaka iz svoje nadležnosti, za njihovu uplatu u proračun te za izvršavanje svih rashoda i izdataka u skladu s namjenama. Takvo određenje, iako vrlo ekstenzivnog obuhvata, predstavlja zakonsku osnovu na temelju koje gradska tijela provode sve postupke i radnje kako bi izvršili utvrđenje, evidentiranje, obračun i (prisilnu) naplatu svih svojih prihoda s jedne, ali i izvršavanje svih rashoda i izdataka, bez obzira na osnovu nastanka, u skladu s namjenama s druge strane.

6. Prava ispitanika u skladu s normativnim okvirom kojim se uređuje zaštita osobnih podataka

Grad je, u skladu s odredbom članka 12. GDPR-a, dužan poduzeti odgovarajuće mjere kako bi se ispitaniku pružile sve informacije iz članaka 13. i 14. i sve komunikacije iz članaka od 15. do 22. te članka 34. u vezi s obradom u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu. Informacije se pružaju u pisanom obliku ili drugim sredstvima, a ako je prikladno, elektroničkim putem. Ako to zatraži ispitanik, informacije se mogu pružiti usmenim putem, pod uvjetom da je drugim sredstvima utvrđen identitet ispitanika.

Voditelj obrade ispitaniku na zahtjev pruža informacije o poduzetim radnjama iz članaka 15. do 22., bez nepotrebnog odgađanja i u svakom slučaju u roku od mjesec dana od zaprimanja zahtjeva. Taj se rok može prema potrebi produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjevâ.

Međutim, važno je naglasiti kako, ako ne postupi po zahtjevu ispitanika, Grad bez odgađanja i najkasnije mjesec dana od primitka zahtjeva, izvješćuje ispitanika o razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženju pravnog lijeka.

S tim u vezi ističemo kako je potrebno, prilikom zaprimanja zahtjeva, nedvojbeno utvrditi identitet ispitanika te, u skladu s objašnjenjem iz članka (62) uvodne izjave GDPR-a, utvrditi posjeduje li ispitanik takvu informaciju.

U slučaju da isti posjeduje takvu informaciju, zatim ako je bilježenje ili otkrivanje osobnih podataka izrijekom propisano zakonom, odnosno ako je pružanje informacije ispitaniku nemoguće ili bi zahtijevalo nerazmjeran napor, obvezu pružanja informacija ipak nije potrebno nametati voditelju obrade. Ovo osobito ako bi pružanje informacija predstavljalo nerazmjeran napor, odnosno ako se obrada obavlja u svrhe arhiviranja u javnom interesu.

7. Obveze Grada Dugog Sela u odnosu na prava ispitanika

a) Pružanje informacija ispitanicima

Prije svega, važno je naglasiti kako je GDPR propis koji uređuje područje zaštite podataka za sve kategorije voditelja i izvršitelja obrade, bez obzira na područje njihova rada, djelatnost ili opseg podataka koje u te svrhe prikupljaju. Kako bi se voditelji i izvršitelji obrade uskladili s GDPR-om, potrebno je poduzeti sljedeće korake i aktivnosti:

- pružanje informacija ispitanicima u svrhu ostvarivanja njihovih prava (članci 12. -21. GDPR-a),
- provođenje odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka (članak 25. i članak 32. GDPR-a),
- vođenje evidencija aktivnosti obrade (članak 30. GDPR-a),
- imenovanje službenika za zaštitu podataka (članak 37. GDPR-a) te
- pružanje informacija u svrhu ostvarivanja prava ispitanika.

S ciljem poštivanja načela transparentnosti, voditelj obrade dužan je ispitaniku pružiti sve informacije o obradi njegovih osobnih podataka u sažetom, razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika te ga upoznati sa njegovim pravima koja mu pripadaju sukladno GDPR-u vezano za obradu njegovih osobnih podataka.

Sažimajući odredbe *supra* citiranih članaka koji se odnose na prava ispitanika, može se zaključiti kako postoje određena univerzalna pitanja na koja je svakako potrebno znati odgovore kako bi Grad mogao pružiti sljedeće informacije ispitanicima:

- o svom identitetu (kontakt podaci voditelja obrade),
- o službeniku za zaštitu podataka (kontakt podaci službenika),
- upoznati ih sa svrhom i pravnom osnovom za obradu osobnih podataka,
- o primateljima ili kategorijama primatelja osobnih podataka (primjerice: HZZO, HZMO),
- *o prenošenju osobnih podataka trećoj zemlji ili međunarodnoj organizaciji (koje nisu članice EU) (nije primjenjivo za Grad),*
- *o legitimnom interesu (nije primjenjivo za Grad),*
- o vremenskom roku pohrane osobnih podataka te kriterijima kojima se utvrđuje razdoblje pohrane,
- o postojanju prava da se od voditelja obrade zatraži pristup osobnim podacima, ispravak, brisanje osobnih podataka ili ograničavanje obrade koja se na njega odnose, prava na ulaganje prigovora na obradu takvih podataka te na prenosivost njegovih podataka drugom voditelju obrade,
- o pravu da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije nego što je ona povučena,
- o pravu na podnošenje prigovora nadzornom tijelu (AZOP),
- je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže,
- *o postojanju automatiziranog donošenja odluka, što uključuje izradu profila te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika (nije primjenjivo za Grad).*

Iako se u smislu pružanja informacija korisnicima navodi kako je potrebno pružiti i informacije o tome prenose li se osobni podaci trećoj zemlji ili međunarodnoj organizaciji (koje nisu članice EU), zatim o postojanju legitimnog interesa, kao i eventualnom postojanju automatiziranog donošenja odluka, držimo kako zbog specifičnog položaja Grada takve mjere nisu primjenjive na poslovanje istog.

Također, držimo važnim naglasiti kako poznavanje svih pravnih osnova za obradu osobnih podataka predstavlja nužan preduvjet kako bi se s vremenom mogle sastaviti i uredno voditi evidencije aktivnosti obrade u smislu članka 30. GDPR-a, ali i pružiti sve relevantne informacije nadzornim i drugim tijelima (e. g. nadležnim sudovima) s ciljem otklanjanja mogućnosti za nastup bilo kakvih štetnih posljedica za Grad.

b) Pružanje informacija ispitanicima – praktična primjena

Poznavanje pravnih osnova i temelja za obradu podataka iz portfelja Grada nužan je preduvjet pružanju potpunih informacija ispitaniku u smislu odredbi GDPR-a. Izostanak

poznavanja takvih osnova, a posljedično i propuštanje davanja potrebnih informacija može uzrokovati brojne neželjene posljedice kako za Grad, tako i za nadležne službenike.

U tom je smislu važno razlikovati nekoliko praktično izglednih situacija. U slučaju da se podaci prikupljaju od ispitanika, Grad je dužan u skladu s člankom 14. GDPR-a ispitaniku pružiti sljedeće informacije:

- identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, predstavnika voditelja obrade;
- kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
- svrhe obrade radi kojih se upotrebljavaju osobni podaci, kao i pravnu osnovu za obradu;
- ako se obrada temelji na članku 6. stavku 1. točki (f), legitimne interese voditelja obrade ili treće strane;
- primatelje ili kategorije primatelja osobnih podataka, ako ih ima;
- ako je primjenjivo, činjenicu da voditelj obrade namjerava osobne podatke prenijeti trećoj zemlji ili međunarodnoj organizaciji;
- razdoblje u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterije kojima se utvrdilo to razdoblje;
- postojanje prava da se od voditelja obrade zatraži pristup osobnim podacima i ispravak ili brisanje osobnih podataka ili ograničavanje obrade koji se odnose na ispitanika ili prava na ulaganje prigovora na obradu takvih te prava na prenosivost podataka;
- ako se obrada temelji na privoli, o postojanju prava da se privola povuče;
- informaciju o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili uvjet nužan za sklapanje ugovora te ima li ispitanik obvezu pružanja osobnih podataka i koje su moguće posljedice ako se takvi podaci ne pruže;
- postojanje automatiziranog donošenja odluka.

Međutim, u skladu sa *supra* navedenim, ako ispitanik već raspolaže takvim informacijama, navedene informacije istom nije potrebno pružiti.

Nadalje, u slučajevima da se podaci ne prikupljaju od ispitanika, a koje situacije, obzirom da Grad obavlja poslove nužne za izvršavanje zadaće od javnog interesa ili pri izvršavanju svojih službenih ovlasti, svakako pretežu u poslovanju Grada, pored naprijed navedenog potrebno je još navesti (ako je primjenjivo) kategorije te informacije o izvoru osobnih podataka. Ako su podaci dostupni iz javno dostupnih izvora, tu je okolnost potrebno naznačiti.

Kako bi se pojednostavilo poslovanje, a pritom ispunile sve obveze u smislu GDPR-a, predlaže se navedene informacije predati na obrascu ili formularu za ostvarivanje određenog prava.

- **Pravo na pristup**

Ispitanik ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i sljedećim informacijama:

- svrsi obrade,
- kategorijama osobnih podataka o kojima je riječ,

- primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni,
- ako je to moguće, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja,
- postojanju prava da se od voditelja obrade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika ili prava na prigovor na takvu obradu,
- pravu na podnošenje pritužbe nadzornom tijelu,
- ako se osobni podaci ne prikupljaju od ispitanika, svakoj dostupnoj informaciji o njihovu izvoru te
- postojanju automatiziranog donošenja odluka.

Grad je dužan, s ciljem osiguravanja prava na pristup, osigurati kopiju osobnih podataka koji se obrađuju, uz napomenu kako za to može naplatiti razumnu naknadu na temelju eventualnih administrativnih troškova.

- **Pravo na ispravak**

Ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose te dopuniti nepotpune osobne podatke, uz napomenu kako valja voditi računa zadire li se time u valjanost javnih isprava, odnosno upravnih i drugih akata protiv kojih više nije moguće izjaviti pravni lijek.

- **Pravo na brisanje**

Iako je upravo ovo pravo u žarištu pažnje šire javnosti i medija koji su obavještavali o GDPR-u, valja istaknuti kako Grad obrađuje podatke radi poštivanja svojih pravnih obveza, za izvršavanje službenih ovlasti i zadaća od javnog interesa te u svrhu arhiviranja u javnom interesu, u kojem slučaju odredbe članka 17. GDPR-a o brisanju osobnih podataka u pravilu nisu primjenjive na Grad kao voditelja obrade.

- **Pravo na prigovor**

Ispitanik ima pravo, na temelju svoje posebne situacije, u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega ako je obrada nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade. Prigovor se podnosi nadležnom tijelu, odnosno AZOP-u.

c) O privoli

Iako privola ispitanika predstavlja tek jednu od osnova za zakonitu obradu osnovnih podataka, čini se da u široj stručnoj javnosti prevladava mišljenje kako je riječ o jedinoj osnovi prema kojoj se prikupljaju podaci ispitanika. Uvažavajući odredbe *supra* navedenog članka 6. GDPR-a te okolnost da Grad gotovo sve podatke prikuplja s ciljem izvršavanja zadaće od javnog interesa ili pri izvršavanju službenih ovlasti, ipak postoji mogućnost da se neki podaci mogu prikupljati na temelju privole.

U tom smislu je potrebno naglasiti kako privola mora sadržavati izričitu suglasnost da se podaci mogu obrađivati u točno navedenu svrhu, a istu okolnost mora biti moguće dokazati.

Dakle, predlaže se tekst privole inkorporirati u prijavnice, obrasce ili druge suglasnosti koje će ispitanik osobno potpisati, odnosno na temelju kojih će se nedvojbeno moći dokazati da je isti dao privolu za obradu svojih osobnih podataka. Naveden obrasci priložit će se u odgovarajuće spise. Također, ispitanik se mora obavijestiti o tome da može u svakom trenutku povući privolu.

Budući da upravni odjeli Grada u svom poslovanju provode niz natječaja ili javnih poziva za dodjelu različitih potpora ili naknada, a u slučaju da je zakonom ili općim aktima kojima je uređena dodjela takvih potpora ili naknada propisano da se pojedinačni akti u kojima se navode osobe kojima su dodijeljena takva sredstva javno objavljuju, tada takav propis, odnosno opći akt predstavlja valjanu osnovu za objavu osobnih podataka.

Međutim, uvijek valja voditi računa da se ne objavljuju podaci koji nisu nužni za ispunjenje svrhe informiranja javnosti o trošenju proračunskih sredstava, a u slučaju da se objavljuju službeni dokumenti ili obrasci koji sadrže veći opseg osobnih podataka, iste je potrebno anonimizirati ili jednostavno precrtati.

d) O certificiranju

Kako bi se povećala transparentnost i usklađenost s GDPR-om, trebalo bi se poticati uvođenje mehanizama certificiranja te pečata i oznaka za zaštitu podataka, što bi ispitanicima, odnosno korisnicima omogućilo jasan uvid u poslovanje Grada u odnosu na osobne podatke koje prikuplja. Drugim riječima, takvim bi se mehanizmima dokazalo postojanje odgovarajućih mjera zaštite koje osiguravaju voditelji obrade i izvršitelji obrade.

Iz odredbi članka 43. GDPR-a proizlazi kako akreditaciju za takvo certificiranje mogu dati AZOP i nacionalno akreditacijsko tijelo imenovano u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća (20) u skladu s EN-ISO/IEC 17065/2012, odnosno Hrvatska akreditacijska agencija. U vrijeme nastanka ove Strategije takvo certificiranje u Republici Hrvatskoj nije uspostavljeno, slijedom čega se može zaključiti kako se predmetni mehanizmi s vremenom trebaju definirati, a potom i primjenjivati u praktičnom radu širokog kruga različitih voditelja i izvršitelja obrade osobnih podataka.

Međutim, držimo važnim istaknuti kako pribavljanje certifikata od strane nadležnih tijela u skladu s navedenim, iako u skladu s odredbom članka 24. stavka 3. GDPR-a dokazuje usklađenost poslovanja voditelja obrade s normativnim okvirom, ne umanjuje odgovornost voditelja obrade ili izvršitelja obrade za poštovanje GDPR-a, slijedom čega je, čak i u slučaju pribavljanja odgovarajućeg certifikata, svakako poželjno izvršavati sve propisane obveze u smislu zaštite osobnih podataka.

8. Organizacijske mjere zaštite osobnih podataka

Grad je, kao voditelj obrade osobnih podataka, dužan u skladu s odredbom članka 24. GDPR-a provoditi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s Uredbom, a te se mjere prema potrebi preispituju i

ažuriraju. Takva neodređena formulacija ne daje jasan odgovor na pitanje što su točno organizacijske mjere, odnosno koje konkretne organizacijske mjere je voditelj obrade dužan poduzeti kako bi osigurao, a kasnije i mogao dokazati, svoju usklađenost s propisima kojima se uređuje pitanje zaštite osobnih podataka.

Organizacijske mjere zaštite trebale bi osigurati da se podaci koje voditelj obrade obrađuje, obrađuju u skladu s naprijed navedenim načelima obrade osobnih podataka u smislu članka 5. GDPR-a.

Budući da je voditelj obrade, u skladu sa stavkom 2. *supra* navedenog članka, odgovoran za usklađenost obavljanja svojih djelatnosti koje uključuju obradu osobnih podataka, potrebno je poduzeti određene mjere kako bi se isti obrađivali u skladu s navedenim načelima. Takve mjere odnose se u najširem smislu na sve gradske službenike čije profesionalne obveze u okviru njihovih radnih mjesta zahtijevaju obradu osobnih podataka. Također, izrazito je važno napomenuti kako se opisane mjere, osim na službenike, namještenike i vježbenike, odnose i na sve stručne suradnike, druge ugovorne strane, kao i sve osobe koje dolaze u doticaj s osobnim podacima u okviru stručnog ili sličnog usavršavanja u Gradu.

Stoga, a u skladu s preporukama AZOP-a, Grad bi, s obzirom na vrstu podataka te uvažavajući zakonitost prikupljanja istih, trebao poduzeti sljedeće organizacijske mjere univerzalne primjenjivosti na sve ustrojstvene jedinice u Gradu:

- dokumentaciju u papirnatom obliku, koja sadrži osobne podatke, voditelj obrade dužan je pohraniti, primjerice u prostorije, ormare ili ladice pod ključem koji će biti pod nadzorom ovlaštenih osoba voditelja obrade;
- pristup osobnim podacima pohranjenim u elektroničkom obliku trebao bi biti omogućen uporabom korisničkog imena i lozinke, bez obzira na programska rješenja koja se koriste u radu;
- potpisivanje izjava o povjerljivosti osoba koje su u obradi osobnih podataka.

Nadalje, iako je svakako za preporučiti poduzimanje mjera kojima se osigurava pravodobna ponovna uspostava dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta (kolokvijalno *backup* podataka), iz odredbi GDPR-a ne proizlazi nedvojbeno kako su voditelji dužni osiguravati takve mjere.

Navedene je mjere potrebno primijeniti na sve evidencije i područja rada, bez obzira jesu li u papirnatom ili digitalnom obliku, za sve ustrojstvene jedinice koje u okviru svog rada obrađuju osobne podatke ispitanika.

Pravno uporište za provođenje naprijed navedenih radnji deriviramo iz odredbe članka 24. stavka 1. i članka 25. stavka 2. GDPR-a koji glase:

„Članak 24.
Obveze voditelja obrade

1. Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju.

Članak 25.

Tehnička i integrirana zaštita podataka

2. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.“

Iz citiranih odredbi GDPR-a proizlazi u bitnome kako su svi voditelji obrade dužni provoditi odgovarajuće tehničke i organizacijske mjere zaštite koje se prema potrebi preispituju i ažuriraju, a takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinaca. Dakle, za navedene norme (kao i za većinu odredbi GDPR-a) možemo reći kako su nesavršene i prilično neodređene te da je, s ciljem pronalaženja i utvrđivanja pravog sadržaja i smisla navedenih normi, iste potrebno tumačiti na način da se promatraju u međuovisnom kontekstu cilja koji se njihovom primjenom nastoji postići u odnosu na specifičnu zakonsku osnovu na temelju koje Grad kao voditelj obrade obrađuje osobne podatke ispitanika.

Budući da Grad obrađuje osobne podatke pojedinaca s ciljem izvršavanja zadaća u javnom interesu, odnosno pri izvršavanju službene ovlasti, odgovor na pitanje je li potrebno posebno navoditi sve propise za svaku pojedinačnu obradu nalazimo u odredbi članka (45) Uvodne izjave GDPR-a koja glasi:

„Ovom se Uredbom ne zahtijeva potreba posebnog propisa za svaku pojedinačnu obradu. Jedan propis kao osnova za više postupaka obrade, koji se temelje na pravnoj obvezi kojoj podliježe voditelj obrade ili ako je obrada potrebna za izvršenje zadaće koja se provodi zbog javnog interesa ili pri izvršavanju službene ovlasti, može biti dovoljan.“

Stoga, uvažavajući prethodno citiranu odredbu GDPR-a te okolnost kako ZLP(R)S svakako predstavlja temeljni propis kojim je uređeno područje lokalne i područne (regionalne) samouprave u Republici Hrvatskoj na temelju kojeg se donose brojni materijalnopravni propisi kojima se detaljno razrađuju upravna i druga područja u nadležnosti Grada, držimo kako se navođenjem istoga daje odgovor na pitanje o tome koja je pravna osnova na temelju koje Grad obrađuje osobne podatke pojedinaca.

Također, držimo kako bi česte izmjene normativnog okvira i istovremena primjena različitih općih i posebnih pravnih instituta uređenih brojnim posebnim propisima, na poslovanje Grada, učinile dosljedno navođenje svakog pojedinačnog propisa za svaku pojedinačnu obradu podataka praktično nemogućim.

a) Organizacijske mjere zaštite u odnosu na službeničke i radnopravne odnose

Radnopravni odnosi u Gradu kao jedinici lokalne samouprave uređeni su, prije svega, Zakonom o službenicima i namještenicima u lokalnoj i područnoj (regionalnoj) samoupravi ("Narodne novine", broj 86/08, 61/11 i 04/18; u daljnjem tekstu: ZSNLP(R)S), dok se u skladu s odredbom članka 3. stavka 3. citiranog Zakona, na pitanja koja nisu uređena istim primjenjuju opći propisi o radu. Nadalje, u smislu obrade osobnih podataka, Grad je, u skladu s odredbama Pravilnika o sadržaju i načinu vođenja evidencije o radnicima ("Narodne novine", broj 73/17), dužan voditi Evidencije o radnicima i radnom vremenu koje sadrže posebne kategorije osobnih podataka (članak (53) Uvodne izjave i članak 9. GDPR-a).

Poslodavac Evidenciju o radnicima počinje voditi datumom zasnivanja radnog odnosa i ažurno je vodi do prestanka radnog odnosa te istu čuva kao dokumentaciju trajne vrijednosti.

Također, u okviru poštivanja svojih zakonskih obveza u skladu s propisima kojima se uređuje područje poreza te mirovinskog i zdravstvenog osiguranja, Grad određene podatke dostavlja tijelima u sustavu državne uprave (Hrvatski zavod za mirovinsko osiguranje, Hrvatski zavod za zdravstveno osiguranje, Hrvatski zavod za zapošljavanje, Porezna uprava i druga tijela u okviru svojih na zakonu utemeljenih ovlasti) kao primateljima obrade u smislu članka 4. stavka 1. točke 9. GDPR-a.

O prijmu i rasporedu službenika na radna mjesta u skladu s aktima kojima se uređuje ustrojstvo Grada, odlučuje se rješenjem u upravnom postupku na temelju citiranog ZSNLP(R)S. Također, na temelju članka 117. i članka 118. istog Zakona, upravni odjeli lokalnih jedinica dužni su voditi osobne očevidnike službenika i namještenika koji su zaposleni u upravnim tijelima lokalne jedinice.

U pogledu natječajne dokumentacije ističemo odredbe *Općeg popisa gradiva s rokovima čuvanja* kojeg na temelju članka 9. Pravilnika o vrednovanju te postupku odabiranja i izlučivanja arhivskog gradiva donosi Hrvatsko arhivsko vijeće na prijedlog Hrvatskog državnog arhiva.

b) Organizacijske mjere zaštite u odnosu na pohranu, prijenos i dostupnost korisničkih podataka

Osobne podatke fizičkih osoba u okviru svojih radnih mjesta obrađuju službenici Grada, ali i treće osobe u skladu sa zakonskim ili ugovornim odnosima sklopljenim s Gradom kao voditeljem obrade.

Poslovanje u digitalnom obliku, bez obzira na potrebe vođenja dokumentacije i poslovanja u skladu s važećom Uredbom o uredskom poslovanju, danas možemo promatrati kao nezaobilazni poslovni standard, i to bez obzira je li riječ o privatnom ili javnom sektoru. Gotovo je nezamislivo da se sve veća količina podataka kojima Grad u svom poslovanju raspolaže obrađuje bez uporabe različitih informacijskih tehnologija, bilo da takve podatke obrađuju i pohranjuju sami službenici Grada na svojim računalima koja koriste u poslovne svrhe, bilo da ih povjeravaju određenim izvršiteljima obrade. Stoga je, slijedom navedenoga, izrazito preporučljivo provoditi mjere opisane u točki 9. ove Strategije u svim ustrojstvenim jedinicama Grada koje u okviru svog djelokruga obrađuju osobne podatke korisnika.

c) Potreba izrade općih i pojedinačnih akata kojima se ostvaruju organizacijske mjere zaštite osobnih podataka

Preporučljivo je uskladiti interne akte vezane uz radnopravne, odnosno službeničke odnose na način da isti sadrže odredbe kojima se službenici i namještenici u okviru svojih radnih mjesta obvezuju na zaštitu osobnih podataka koji se odnose na ispitanike. Međutim, obzirom na specifičnosti Grada kao jedinice područne samouprave, postavlja se pitanje na koji način implementirati odredbe koje se odnose na obveze službenika i namještenika u smislu zaštite osobnih podataka, a poštujući pritom odredbe postojećeg normativnog okvira.

Nastavno na navedeno, posebno se ističu dvije mogućnosti u okviru kojih je moguće urediti predmetno pitanje.

S jedne strane, može se pristupiti izradi standardiziranog obrasca izjave o povjerljivosti koje bi se uručile svakom službeniku (i namješteniku) na potpis, a kojima bi se isti obvezali čuvati povjerljivost svih osobnih podataka kojima imaju pravo i ovlast pristupa, da će osobne podatke koristiti isključivo u točno određenu svrhu, kao i da iste neće učiniti dostupnima trećim osobama.

S druge strane, potrebno je uvažiti odredbu članka 4. ZSNLP(R)S na temelju koje su jedinice lokalne i područne (regionalne) samouprave dužne donijeti pravilnike o unutarnjem redu kojima se utvrđuje unutarnje ustrojstvo upravnih tijela, nazivi i opisi radnih mjesta, stručni i drugi uvjeti za raspored na radna mjesta, broj izvršitelja, ali i druga pitanja od značaja za rad upravnih tijela u skladu sa statutom i drugim općim aktima.

Budući da ne postoji izravna zakonska ovlast koja gradska tijela ovlašćuje na donošenje akata kojima se uređuje zaštita osobnih podatka, držimo kako je predmetno pitanje preporučljivo riješiti na naprijed opisani način, i to uvažavajući postojeće važeće propise kojima se uređuju organizacijski i radnopravni odnosi u Gradu.

d) Izvršitelji obrade

Uslijed povećanog opseg poslova, nedostatka određenih stručnih znanja, kao i nedostatnih financijskih i/ili administrativnih kapaciteta, voditelji obrade često povjeravaju obavljanje određenih poslova iz svoje nadležnosti trećim pravnim subjektima specijaliziranima upravo za obavljanje takvih poslova. Također, zbog brzog tehnološkog razvoja i informatizacije poslovanja tijelima javne vlasti omogućuje se uporaba osobnih podataka u do sada nedosegnutom opsegu, što svakako generira nove izazove u području zaštite osobnih podataka.

U skladu s definicijom iz članka 4. stavka 1. točke 8. GDPR-a, izvršitelj obrade može biti fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Kao primjere izvršitelja obrade navodimo knjigovodstvene servise koji obrađuju podatke o plaćama radnika za poslodavca, zatim trgovačka društva za pružanje zaštitarskih usluga ili usluga video nadzora u okviru istih, kao i pružanje širokog spektra usluga koje koriste informacijske tehnologije za obavljanje poslova iz nadležnosti voditelje obrade.

U slučaju angažiranja izvršitelja obrade, Grad osobito vodi računa kako se u skladu s GDPR-om dužan koristiti jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz GDPR-a i da se njome osigurava zaštita prava ispitanika. Obrada koju provodi izvršitelj obrade uređuje se ugovorom ili drugim pravnim aktom u skladu s pravom Unije ili pravom države članice koji izvršitelja obrade obvezuje prema voditelju obrade, a koji navodi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te druge obveze i prava voditelja obrade u smislu odredbe članka 28. GDPR-a.

9. O tehničkim mjerama zaštite osobnih podataka

U skladu s citiranim odredbama GDPR-a u točki 8. ove Strategije, Grad, pored organizacijskih, provodi i tehničke mjere zaštite. Takvim mjerama osigurava se da podaci, sukladno naprijed rečenom, nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca. U tom smislu, a nastavno na navode i preporuke AZOP-a, valja voditi računa kako bi pristup osobnim podacima pohranjenim u elektroničkom obliku trebao biti omogućen uporabom korisničkog imena i lozinke.

Također, preporučuje se, gdje je moguće i primjenjivo, izraditi sigurnosne kopije podataka kako bi se na odgovarajući način osigurala sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta.

Uvažavajući okolnost kako je GDPR tehnološki neutralan propis te kako ne propisuje konkretna informacijska rješenja u tom smislu, preporuča se provođenje mjera zaštite kojima se, u skladu s dostupnim IT rješenjima, može osigurati da podaci nisu automatski dostupni trećim osobama. Navedeno se svakako odnosi na pohranu podataka u elektroničkom obliku, ali je preporučljivo zaštititi na odgovarajući način i svu elektroničku komunikaciju, odnosno pristupe istoj iz razloga što može sadržavati osobne podatke ispitanika, kako unutar Grada tako i prema trećim stranama.

U ovom smislu važno je istaknuti kako GDPR ne daje konkretne informacije o vrsti i obliku tehničkih mjera zaštite, već navodi traženi učinak koji je u smislu zaštite osobnih podataka takvim mjerama potrebno postići, slijedom čega se u nastavku navodi odredba članka (15) Uvodne izjave GDPR-a:

„Radi sprečavanja stvaranja ozbiljnog rizika zaobilaženja propisa, zaštita pojedinaca trebala bi biti tehnološki neutralna i ne bi smjela ovisiti o upotrebljavanim tehnologijama. Zaštita pojedinaca trebala bi se primjenjivati na obradu osobnih podataka automatiziranim sredstvima, kao i na ručnu obradu, ako su osobni podaci pohranjeni ili ih se namjerava pohraniti u sustav pohrane. Dokumenti ili skupovi dokumenata, kao i njihove naslovne stranice, koji nisu strukturirani prema posebnim mjerilima ne bi trebali biti obuhvaćeni područjem primjene ove Uredbe.“

10. Službenik za zaštitu osobnih podataka

U skladu s odredbom članka 37. stavka 1. točke (a) GDPR-a, voditelj obrade dužan je imenovati službenika za zaštitu podataka u svakom slučaju u kojem obradu provodi tijelo javne vlasti ili javno tijelo. Zakonom o provedbi Opće uredbe o zaštiti podataka ("Narodne novine", broj 42/18; u daljnjem tekstu: ZPOUZP) pobliže se definira sintagma *tijela javne vlasti*; u smislu Zakona to su tijela državne uprave i druga državna tijela te jedinice lokalne i područne (regionalne) samouprave. Slijedom navedenog, proizlazi da je Grad svakako dužan imenovati službenika za zaštitu osobnih podataka**.**

Nadalje, a u skladu s citiranim člankom, službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz članka 39. koje se u nastavku navode:

- informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka,

- praćenje poštovanja Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije,
- pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35.,
- suradnja s nadzornim tijelom,
- djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. te savjetovanje, prema potrebi, o svim drugim pitanjima.

Nadalje, službenik za zaštitu osobnih podataka može biti zaposlenik Grada, ali službenikom može biti imenovana i osoba koja nije zaposlenik na temelju ugovora o djelu kao vanjski službenik. Prilikom imenovanja službenika potrebno je voditi računa da takva osoba ne sudjeluje u donošenju odluka kojima se utvrđuje svrha i način obrade osobnih podataka.

Međutim, ni GDPR ni ZPOUZP ne daju izravan odgovor na pitanje o konkretnim stručnim kvalifikacijama službenika, tako da se može zaključiti kako za imenovanje istog ne postoje prepreke koje bi proizlazile s osnova razine stručne spreme ili zvanja. Također, istim propisima određeno je kako je pri imenovanju službenika za zaštitu osobnih podataka potrebno voditi računa o njegovim stručnim kvalifikacijama, ali nije definirano koje su to stručne kvalifikacije te na koji način se iste mogu provjeriti.

Također, odredbom članka 38. stavka 6. GDPR-a određeno je kako voditelj obrade ili izvršitelj obrade osigurava da zadaće i dužnosti službenika ne dovedu do sukoba interesa. Nadalje, u točki 3.5. Smjernice o službenicima za zaštitu podataka Radne skupina osnovane na temelju članka 29. Direktive 95/46/EZ navodi se da službenik za zaštitu podataka ne može biti djelatnik organizacije čiju svrhu i načine obrade osobnih podataka mora utvrditi.

11. Isključenje primjene upravne novčane kazne u odnosu na tijela javne vlasti

Nastavno na navedeno u prethodnoj točki, nije dvojbeno da je Grad tijelo javne vlasti u smislu ZPOUZP-a. Odredbom članka 47. istog Zakona propisano je kako se u postupcima koji se provode protiv tijela javne vlasti, tijelu javne vlasti ne može se izreći upravna novčana kazna za povrede ZPOUZP-a ili GDPR-a.

Međutim, s obzirom na niz drugih ovlasti nadzornog tijela s osnova članka 58. GDPR-a, takva se formulacija ni u kom slučaju ne može tumačiti na način da općine i gradovi nisu obveznici primjene GDPR-a i drugih propisa te smjernica kojima se uređuje područje zaštite osobnih podataka. S tim u vezi, nedvojbeno je kako je Grad dužan poduzeti mjere kojima se postiže usklađenost, odnosno obveza poštivanja prava i izvršenja obveza s navedenim normativnim okvirom.

12. Umjesto zaključka

Grad je, uvažavajući sve svrhe radi kojih je i ustrojen, a tako i poslove koje u okviru svojih javnopravnih ovlasti obavlja, svakako voditelj obrade osobnih podataka za izrazito širok raspon korisnika (ispitanika u smislu GDPR terminologije). Osobni podaci nalaze se i obrađuju u gotovo svim ustrojstvenim jedinicama, a iste, s obzirom na svoje zadaće i funkciju, osobne podatke koriste na različite načine.

Primjera radi, navodimo situacije u kojima se dodjeljuju određena sredstva ili utvrđuju obveze za sve korisnike, a tako i fizičke osobe. Bez obzira je li riječ u upravnom ili neupravnom postupku ili pravnom poslu, kao i okolnosti postupa li se po službenoj dužnosti ili na zahtjev stranke, prije svega je u kontekstu uredskog poslovanja potrebno evidentirati i otvoriti predmet za tu namjenu, a zatim isti dodijeliti nadležnom upravnom tijelu ili službeniku.

Nadalje, pojedinačni akt kojim se utvrđuje određeno pravo ili obveza potrebno je u pravilu putem pisarnice dostaviti naslovljenoj osobi, uglavnom putem vanjskog izvršitelja poštanskih usluga. Obzirom da je riječ o određenom pravu ili obvezi financijske naravi, istu je obvezu potrebno pravilno evidentirati u poslovnim knjigama, sastaviti odgovarajuće knjigovodstvene isprave te izvršiti plaćanje, odnosno radnje usmjerene na naplatu istih, dok je neke isprave ili akte potrebno dostaviti drugim javnopravnim tijelima kao primateljima obrade. Konačno, upravne i neupravne spise kojima se izravno ili neizravno odlučuje o pravima i obvezama fizičkih osoba potrebno je arhivirati u skladu s navedenim u točki 3. e. ove Strategije.

Stoga, s ciljem postizanja usklađenosti poslovanja Grada s normativnim okvirom kojim se uređuje područje zaštite osobnih podataka, odnosno poduzimanja svih radnji kako bi se pravilno izvršila sva prava i obveze u tom smislu, u nastavku ukratko ponavljamo one aktivnosti za koje držimo kako će omogućiti postizanje takve usklađenosti, odnosno izvršenja prava i obveza.

Nastavno na naprijed navedeno, a budući da će potencijalni upiti od strane korisnika ili nadzornog tijela biti adresirani na Grad kao funkcionalnu i organizacijsku cjelinu, potrebno je jednim dokumentom sažeti te navesti čitko i razumljivo one bitne elemente pomoću kojih će se zadovoljiti tehničke i organizacijske mjere zaštite, a potom i olakšati pružanje svih bitnih i relevantnih informacija u vezi ostvarivanja prava ispitanika.

Naveden je normativni okvir prema kojem se dokazuje zakonitost prikupljanja podatka, opisane su mjere kojima se, uvažavajući osobito okolnost da je Grad tijelo javne vlasti, postiže organizacijska i tehnička usklađenost s GDPR-om, izrađene su formulacije, gdje je primjenjivo, univerzalnih odgovora na upite korisnika, utvrđena je obveza imenovanja službenika za zaštitu osobnih podataka te su izrađeni nacrti akata koje je potrebno javno objaviti te dostaviti nadležnom tijelu.

Zaključno, s obzirom da se može zaključiti kako u vrijeme nastanka ove Strategije normativni okvir nije konačan te se mogu očekivati različite upute i obvezujuća mišljenja nadležnih tijela, ovu Strategiju valja promatrati kao niz smjernica za usklađivanje poslovanja Grada u području zaštite osobnih podataka te razvijati svijest o tome kako će pojedine mjere i postupke biti potrebno i dalje ažurirati te usklađivati u skladu s praksom naprijed navedenih nadležnih tijela.

KLASA: 023-05/19-01/05
URBROJ: 238/07-01-04/01-02-19-2

Gradonačelnik
Grada Dugog Sela

Dugo Selo, 10. travnja 2019. god.

Nenad Panian, dr. med. dent.,v.r.