Na temelju odredbe članka 3. stavka 1. 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 stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i članka 9. Statuta Državnog ureda za reviziju, KLASA: 012-03/19-01/1, URBROJ: 613-01-01-19-1, od 19. rujna 2019., glavni državni revizor donosi

PRAVILNIK O OBRADI I ZAŠTITI OSOBNIH PODATAKA

DRŽAVNOG UREDA ZA REVIZIJU

1. OPĆE ODREDBE

Članak 1.

1. Državni ured za reviziju (dalje u tekstu: Ured) obveznik je primjene odredbi 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 stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (dalje u tekstu: Opća uredba

o zaštiti podataka).

1. Ovim Pravilnikom utvrđuju se načini i mjere te pravila kojih se Ured, zaposlenici zaduženi za obradu i zaštitu osobnih podataka te izvršitelji obrade pridržavaju prilikom prikupljanja, obrade i čuvanja svih vrsta i skupina osobnih podataka kako bi Ured ispunio svoje obveze propisane Općom uredbom o zaštiti podataka, a sve u skladu sa Zakonom o provedbi Opće uredbe o zaštiti podataka (Narodne novine 42/18).
2. Ovim Pravilnikom se utvrđuje koji se podaci smatraju osobnim podatkom, kao i mjere za obradu, čuvanje i priopćavanje osobnih podataka.
3. Riječi i pojmovi koji se koriste u ovom Pravilniku, a koji imaju rodno značenje, bez obzira na to jesu li korišteni u muškom ili ženskom rodu, odnose se na jednak način na muški i ženski rod.

Članak 2.

Pojedini izrazi u ovom Pravilniku imaju sljedeće značenje:

1. „Osobni podaci” – svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.
2. „Ispitanik” – pojedinac čiji se identitet može utvrditi; 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.
3. „Izvršitelj obrade” – fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime Ureda.
4. „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.
5. „Ograničavanje obrade” – označavanje pohranjenih osobnih podataka u cilju ograničavanja njihove obrade u budućnosti.
6. „Pseudonimizacija” – 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.
7. „Sustav pohrane” – svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.
8. „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 Europske unije ili pravom države članice, voditelj obrade ili posebni kriterij za njegovo imenovanje mogu se predvidjeti pravom Europske unije ili pravom države članice.
9. „Primatelj” – fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana.
10. „Treća strana” – fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osoba koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade.
11. „Privola ispitanika” – svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želje ispitanika kojom on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.
12. „Povreda osobnih podataka” – kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.
13. „Nadzorno tijelo” je Agencija za zaštitu osobnih podataka.

Članak 3.

Ured je voditelj obrade osobnih podataka kojima samostalno ili s drugima određuje svrhu i sredstva obrade osobnih podataka u skladu s nacionalnim zakonodavstvom ili pravom Europske unije.

Članak 4.

1. Ured osobne podatke obrađuje zakonito, pošteno i transparentno s obzirom na ispitanike i njihova prava.
2. Obrađuju se samo primjereni i relevantni osobni podaci, i to isključivo u posebne, izričite i zakonite svrhe te se dalje ne obrađuju na način koji nije u skladu s tim svrhama.
3. Osobni podaci koje Ured obrađuje su točni te se po potrebi ažuriraju. Osobni podaci koji nisu točni bez odlaganja se brišu ili ispravljaju.
4. Ured osobne podatke obrađuje isključivo 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 i organizacijskih mjera.
5. Ured osobne podatke čuva u obliku koji omogućuje identifikaciju ispitanika i to samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Iznimno, osobni podaci mogu se pohraniti i na dulja razdoblja, ali samo ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

II. OBRADA OSOBNIH PODATAKA

Članak 5.

Ured osobne podatke obrađuje samo ako je ispunjen jedan od sljedećih uvjeta:

1. da je ispitanik dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
2. da je obrada nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije zaključivanja ugovora
3. da je obrada nužna radi poštovanja pravnih obveza Ureda
4. da je obrada nužna kako bi se zaštitili interesi ispitanika ili druge fizičke osobe
5. da je obrada nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službenih

ovlasti Ureda

1. da je obrada nužna za potrebe legitimnih interesa Ureda ili treće strane, osim u slučaju kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka.

Članak 6.

1. Privola kojom ispitanik Uredu daje pristanak za obradu osobnih podataka koji se na njega odnose mora biti dobrovoljna, nedvosmislena, u pisanom, razumljivom te lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika, jasno naznačenom svrhom za koju se daje i bez nedopuštenih uvjeta.
2. Ispitanik ima pravo u svakom trenutku povući svoju privolu, a povlačenje privole mora biti jednako jednostavno kao i njezino davanje.

Članak 7.

U postupku obrade osobnih podataka Ured na odgovarajući način (pisano ili izravno usmeno) ispitaniku pruža sve informacije vezano za obradu njegovih osobnih podataka, a osobito o svrsi obrade podataka, pravnoj osnovi za obradu podataka, legitimnim interesima Ureda, namjeri predaje osobnih podataka trećim osobama, razdoblju u kojem će osobni podaci biti pohranjeni, o postojanju prava ispitanika na pristup osobnim podacima te na ispravak ili brisanje osobnih podataka i ograničavanje obrade, prava na ulaganje prigovora i drugo.

III. PRAVA ISPITANIKA I ZAŠTITA PRAVA

Članak 8.

1. Ispitanik ima pravo biti informiran o svrsi obrade njegovih osobnih podataka, kategorijama osobnih podataka koji se obrađuju, o primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni te u slučaju kada se osobni podaci ne prikupljaju od ispitanika o njihovu izvoru.
2. Ispitanik ima pravo na pristup podacima podataka sadržanih u sustavu pohrane Ureda koji se na njega odnose.
3. Ispitanik ima pravo na ispis podataka sadržanih u sustavu pohrane Ureda koji se na njega odnose.
4. Ispitanik ima pravo zahtijevati ispravak pogrešno unesenih podataka. U slučaju pogrešno unesenih podataka, Ured će na temelju zahtjeva ispitanika ispraviti pogrešno unesene podatke, odnosno nadopuniti ih.
5. Ured će bez odgađanja, na temelju zahtjeva ispitanika, provesti brisanje osobnih podataka koji se na njega odnose pod uvjetom da više nisu nužni u odnosu na svrhe za koje su prikupljeni ili ako ispitanik povuče privolu na kojoj se obrada temelji.
6. U slučaju da Ured utvrdi da su osobni podaci nepotpuni, netočni ili neažurni, dužan ih je dopuniti ili izmijeniti neovisno o zahtjevu ispitanika.
7. Ako Ured radi izvršenja zadaća od javnog interesa ili zadaća javnih tijela ili se prilikom njihove obrade Ured poziva na svoje legitimne interese, ispitanik može podnijeti prigovor protiv takve obrade podataka, ako postoji interes zaštite podataka ispitanika.
8. Ispitanik koji smatra da mu je povrijeđeno neko pravo zajamčeno Općom uredbom o zaštiti podataka ima pravo podnijeti zahtjev za utvrđivanje povrede prava nadzornom tijelu.

IV. SUSTAV POHRANE

Članak 9.

Ured prikuplja i obrađuje osobne podatke:

* kod obavljanja poslova revizije (provjera dokumenata, isprava, izvješća, sustava unutarnjih kontrola, računovodstvenih, financijskih i drugih postupaka te drugih evidencija radi izražavanja mišljenja jesu li godišnji financijski izvještaji sastavljeni u skladu s mjerodavnim financijsko-izvještajnim i pravnim okvirom, postupak ocjenjivanja jesu li aktivnosti, financijske transakcije i informacije u svakom bitnom pogledu u skladu s mjerodavnim propisima kojima se uređuje poslovanje subjekta revizije, postupak ocjenjivanja ostvaruju li se programi, projekti i aktivnosti subjekta revizije učinkovito odnosno prema načelima ekonomičnosti, djelotvornosti i svrsishodnosti i mogu li se poboljšati) te provjera provedbe naloga i preporuka
* kod postupanja po zaprimljenim podnescima svih vrsta
* kod odgovaranja na zahtjev za ostvarivanje prava na pristup informacijama
* kod zapošljavanja u Uredu
* osobne podatke koji se mogu prikupiti u postupcima javne i jednostavne nabave
* kod sudjelovanja na izobrazbama ili stručnim osposobljavanjima koje organizira Ured, bilateralnoj suradnji s drugim VRI-jevima i njihovim strukovnim udrugama (INTOSAI, ERUROSAI), međunarodnim seminarima, radionicama i programima te Twinning projektima u kojima je Ured partner
* osobne podatke koji se obrađuju za zaposlenike i vanjske suradnike
* kod vođenja evidencije dolazaka zaposlenika na posao
* kod vođenja evidencije dolazaka stranaka u Ured
* kod video nadzora u Središnjem uredu Zagreb u svrhu zaštite osoba i imovine
* kod fotografiranja sudionika na radionicama, programima te raznim izobrazbama
* kod objave fotografija na mrežnim stranicama Ureda i Intranetu
* kod korištenja osobnih imena i prezimena zaposlenika u službenim e-adresama.

V. EVIDENCIJA AKTIVNOSTI OBRADE

Članak 10.

1. Evidencija aktivnosti obrade koju je Ured kao voditelj obrade obvezan ustrojiti sadrži najmanje sljedeće informacije:

* podatke za kontakt voditelja obrade i službenika za zaštitu osobnih podataka
* svrhu obrade
* opis kategorija ispitanika i kategorija osobnih podataka
* kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni
* ako je moguće, predviđene rokove za brisanje različitih kategorija osobnih podataka
* opis tehničkih i organizacijskih sigurnosnih mjera za zaštitu podataka.

1. Evidenciju aktivnosti obrade iz stavka 1. ovog članka Pravilnika sastavlja te po potrebi ažurira Pododsjek za kadrovske poslove.

VI. SLUŽBENIK ZA ZAŠTITU OSOBNIH PODATAKA

Članak 11.

1. Glavni državni revizor imenuje službenika za zaštitu osobnih podataka, koji je zaposlenik Ureda.
2. Kontakt podaci službenika za zaštitu osobnih podataka dostupni su na mrežnim stranicama Ureda te se o imenovanom službeniku za zaštitu osobnih podataka obavještava ovlašteno nadzorno tijelo.
3. Službenik za zaštitu osobnih podataka obavlja poslove informiranja i savjetovanja odgovornih osoba Ureda i njegovih zaposlenika koji neposredno obavljaju obradu osobnih podataka o njihovim obvezama iz Opće uredbe o zaštiti podataka, prati poštivanje odredbi Opće uredbe o zaštiti podataka te drugih odredaba koje se odnose na zaštitu osobnih podataka, zaprima i odgovara na upite ispitanika, pruža savjete vezano za zaštitu osobnih podataka te surađuje s nadzornim tijelom.
4. Službenik za zaštitu osobnih podataka dužan je poštivati pravila povjerljivosti svih informacija koje je saznao u obavljanju svoje dužnosti.
5. Službenik za zaštitu osobnih podataka djeluje neovisno i ne smije biti u sukobu interesa.

VII. MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Članak 12.

1. U svrhu sprječavanja neovlaštenog pristupa osobnim podacima koji su pohranjeni u pisanom obliku, osobni podaci se čuvaju u registratorima, u dosjeima koji se nalaze u zaključanim ormarima kojima pristup imaju samo osobe ovlaštene za obradu predmetnih podataka. Podaci pohranjeni na računalima štite se dodjeljivanjem korisničkih imena i lozinki koja je poznata isključivo zaposlenicima zaduženim za obradu i zaštitu osobnih podataka. Podaci sadržani u raznim programskim aplikacijama štite se dodjeljivanjem korisničkih imena i lozinki te čitačima kartica koja je poznata isključivo zaposlenicima zaduženim za obradu i zaštitu osobnih podataka.
2. U svim slučajevima, a posebno u slučaju javnog objavljivanja podataka u skladu sa Zakonom o pravu na pristup informacijama (Narodne novine 25/13, 85/15 i 69/22), Ured u svrhu zaštite osobnih podataka koristi pseudonimizaciju podataka.
3. Zaposlenici zaduženi za obradu i zaštitu osobnih podataka dužni su poduzeti tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka koje su potrebne kako bi se osobni podaci zaštitili od slučajnog gubitka ili uništenja, od nedopuštenog pristupa ili nedopuštene promjene, nedopuštenog objavljivanja i svake druge zlouporabe.
4. Obrada i zaštita osobnih podataka koju provodi izvršitelj obrade u ime Ureda uređuje se ugovorom na temelju kojeg izvršitelj obrade osigurava odgovarajuću razinu sigurnosti s obzirom na rizik.

VIII. OBRADA OSOBNIH PODATAKA PUTEM VIDEO NADZORA

Članak 13.

Video nadzor u Središnjem uredu Zagreb, na adresi Prolaz Jurja Ratkaja 8, 10 000 Zagreb se odnosi na prikupljanje i daljnju obradu osobnih podataka koja obuhvaća stvaranje snimke koja čini ili je namijenjena da čini dio sustava pohrane.

Članak 14.

1. Obrada osobnih podataka putem video nadzora može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba (radi smanjenja izloženosti zaposlenika riziku od razbojstva, provala, nasilja, krađa i sličnih događaja) i imovine, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem video nadzora.
2. Video nadzor se može koristiti kod rekonstrukcije događaja odnosno okolnosti koje su prethodile nastupanju izvanrednog slučaja. Video nadzor se koristi i u svrhu zaštite svih drugih osoba koje se iz bilo kojeg razloga nađu u prostoru pod kontrolom Ureda, kao i njihove imovine.
3. Svaka obrada osobnih podataka dobivenih putem video nadzora smatra se valjanom u slučaju da je svrha obrade bila nužna i opravdana, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem video nadzora.
4. Snimke video nadzora mogu se isključivo koristiti u svrhe koje su utvrđene ovim Pravilnikom.
5. Video nadzorom obuhvaćeni su zajednički prostori koji se odnose na unutarnje hodnike u prizemlju (tri kamere), prvom katu (dvije kamere), drugom katu (jedna kamera) i trećem katu (jedna kamera). Video nadzorom nisu obuhvaćeni prostori stubišta, ulaznog hola, radnih soba, kuhinja te toaletnih prostorija.
6. U Središnjem uredu Zagreb su u svrhu zaštite osoba i imovine, postavljeni detektori pokreta na lokacijama:

* podrum – dva detektora pokreta (hodnik i kuhinja)
* prizemlje – 15 detektora pokreta (hodnici, radne sobe i portirnica)
* prvi kat – tri detektora pokreta (hodnik i server soba)
* drugi kat – tri detektora pokreta (radne sobe i hodnik)
* treći kat – dva detektora pokreta (hodnik).

Članak 15.

1. Ured je dužan označiti da je objekt odnosno pojedina prostorija u njemu pod video nadzorom, a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja.
2. Obavijest iz stavka 1. ovog članka treba sadržavati jednostavnu i lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije:

* da je prostor pod video nadzorom
* podatke o voditelju obrade
* podatke za kontakt putem kojih ispitanik može ostvariti svoja prava.

Članak 16.

1. Sustav video nadzora mora biti zaštićen od pristupa neovlaštenih osoba.
2. Uređaji za snimanje i pohranu snimke video nadzora te prijenosni mediji s izuzetim snimkama video nadzora smještaju se i čuvaju u prostoriji zaštićenoj od neovlaštenog ulaska i drugih mogućih ugroza. Pristup tim prostorijama dopušten je samo ovlaštenoj osobi.
3. Osoba koja obavlja poslove privatne zaštite ima izravan uvid na monitor i/ili u snimke video nadzora na svom radnom mjestu, u sklopu izvršavanja svojih radnih obveza. Ta osoba nema pravo kopirati, brisati, dodavati, snimati ili na bilo koji drugi način mijenjati snimke video nadzora ili ih predavati trećoj strani te ne smije dozvoliti vizualni pregled monitora od video nadzora od strane neovlaštene osobe. Pristup video nadzoru može imati i ovlašteni serviser i održavatelj. Osoba koja obavlja poslove privatne zaštite i/ili servisa odnosno održavanja video nadzora nije zaposlenik Ureda te je kao zaposlenik druge pravne ili fizičke osobe obvezana na povjerljivost osobnih podataka ispitanika.
4. Pristup osobnim podacima prikupljenim putem video nadzora nakon upućenog zahtjeva mogu dobiti nadležna državna tijela u okviru obavljanja poslova iz svojeg zakonom utvrđenog djelokruga. Obrada snimki video nadzora radi se samo prema potrebi, prema pisanom zahtjevu u slučajevima zbog kojih je video nadzor postavljen te ostvarivanja prava ispitanika.
5. Ured podatke prikupljene putem video nadzora obrađuje 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, sukladno propisima koji uređuju područje zaštite osobnih podataka.
6. Glavni državni revizor će posebnom odlukom urediti sva druga pitanja koja se odnose na video nadzor.

Članak 17.

1. Pravo pristupa podacima prikupljenim putem video nadzora ima glavni državni revizor te pomoćnik glavnoga državnog revizora nadležan za informatičke poslove.
2. Osobe iz stavka 1. ovog članka Pravilnika ne smiju koristiti snimke video nadzora suprotno svrsi utvrđenoj u ovom Pravilniku te su obvezani na povjerljivost osobnih podataka.

IX. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 18.

1. Na sva pitanja koja nisu uređena ovim Pravilnikom neposredno se primjenjuju odredbe nacionalnog prava i Opće uredbe o zaštiti podataka.

2. Ovaj Pravilnik stupa na snagu 26. veljače 2024.

GLAVNI DRŽAVNI REVIZOR

mr. Ivan Klešić, dipl. oec., v. r.

KLASA: 026-01/24-04/0002

URBROJ: 613-01-01-24-2

Zagreb, 26. veljače 2024.