CENTAR ZA KULTURU I INFORMACIJE „MAKSIMIR“
Ulica Lavoslava Švarca 18
ZAGREB
OIB: 31407932125

Na temelju članka 30. stavka 1. alineja 2., Statuta Centra za kulturu i informacije „Maksimir“,, Upravno vijeće Centra za kulturu i informacije „Maksimir“, na 9. sjednici od dana 10. listopada 2018., donijelo je sljedeći,

PRAVILA-POLITIKE

POSTUPANJA I OBAVIJESTI O POVREDI OSOBNIH PODATAKA

Uvodna odredba.

Ovaj Pravilnik je donesen, Temeljem uvodne točke 87. i članka 33. i 34. 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 - Opća uredba o zaštiti podataka - General Data Protection Regulation (skraćeno: GDPR) i članka 28. Pravilnika – interne politike o obradi i zaštiti osobnih **Centra za kulturu i informacije „Maksimir“ .**

1. Svrha pravila o obavijesti o povredi osobnih podataka:

Voditelj obrade je obvezan prema odredbama GDPR-a uspostaviti institucionalni okvir osmišljen kako bi se osigurala sigurnost svih osobnih podataka za cijelo vrijeme trajanja obrade, uključujući jasne linije odgovornosti.

Ova politika određuje postupak koji treba slijediti kako bi se osigurao dosljedan i učinkovit uspostavljen pristup upravljanju kod povrede podataka i incidenata sigurnosti informacijskih sustava Voditelja.

Ova pravila se primjenjuju kako bi se pravovremeno otkrila povreda osobnih podataka; identificirale priroda povrede, kategorije ispitanika, kategorije podataka, spriječile ili umanjile eventualne posljedice povrede, poduzele aktivnosti u s cilju sprečavanja daljnjih povreda. Nadalje kako bi ispitanik - pojedinac mogao poduzeti potrebne mjere opreza, u obavijesti o povredi ispitaniku bi trebalo opisati prirodu povrede osobnih podataka kao i preporuke kako bi dotični pojedinac mogao ublažiti potencijalne negativne učinke.

Fokus zahtjeva za obavješćivanjem je potaknuti zadužene osobe voditelja, da odmah djeluju protiv povrede i ako je moguće, oporavljaju ugrožene osobne podatke i zatraže odgovarajuće savjete od nadzornog tijela. Obavještavanje nadzornog tijela u prvih 72 sata može koristiti voditelju da donese odluke o obavješćivanju ili ne obavijesti pojedinaca i da preispita jesu li te odluke ispravne.

Svrha obavještavanja nadzornog tijela nije samo dobivanje smjernica o tome treba li obavijestiti oštećenike. U nekim će slučajevima biti očigledno da će, zbog prirode prekršaja i ozbiljnosti rizika, voditelj morati obavijestiti oštećene osobe bez odlaganja. Na primjer, ako postoji neposredna prijetnja krađe identiteta ili ako se objavljuju posebne kategorije osobnih podataka, trebalo bi djelovati bez nepotrebnog kašnjenja kako bi se spriječilo povreda i prenošenje podataka. U izuzetnim okolnostima, to se može dogoditi čak i prije no što obavijesti nadzorno tijelo.

Obavijest nadzornog tijela ne može poslužiti kao opravdanje za neuspjeh komunikacije.

2. Opseg primjene

Ova se Politika odnosi na sve osobne i osjetljive podatke koje drži Voditelj bez obzira na format.

Ova se politika primjenjuje na sve radnike Voditelja. To uključuje privremeno, povremeno ili agencijsko osoblje i izvođače radova, konzultanata, dobavljača i obrađivača podataka koji rade za, ili u ime Voditelja.

Cilj ove politike je da spriječi sve povrede, kako bi se smanjio rizik povezan s povredama i razmotrilo što je potrebno za osiguranje osobnih podataka i sprječavanje daljnje povrede.

3. Definicije

-Imenovana osoba: Osoba za davanje obavijesti o povredi osobnih podataka imenovana od strane ravnatelja - Povjerenik za zaštitu privatnosti.

-Povreda podataka: Kao dio rješavanja povreda, treba najprije moći prepoznati jedan od oblika povreda. GDPR definira "povrede osobnih podataka" u članku 4. (12) kao:

"Povrede sigurnosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima prenesenim, pohranjenim ili na drugi način obrađenim".

Pri čemu je pojmovno značenje:

"Uništenje" osobnih podataka podrazumijeva: podaci više ne postoje ili više ne postoje u obliku koji je od bilo kakve koristi voditelju.

"Šteta": podaci promijenjeni, oštećeni ili više nisu potpuni.

"Gubitak" osobnih podataka: podaci i dalje mogu postojati, no voditelj je izgubio kontrolu ili pristup ili više nije u posjedu.

„Neovlaštena ili nezakonita obrada“: može uključivati otkrivanje osobnih podataka (ili pristup) primateljima koji nisu ovlašteni primati (ili pristupiti) podacima ili bilo koji drugi oblik obrade koji krši GDPR.

U svrhu ove Politike, povrede sigurnosnih podataka uključuju povrede i sumnjive incidente.

„Incident“ u kontekstu ove Politike je događaj ili akcija koja može ugroziti povjerljivost, integritet ili dostupnost sustava ili podataka, bilo slučajno ili namjerno, koji bi prouzročio ili ima potencijal da nanese štetu na informacijskim sredstvima Voditelja i/ili ugled.

Incident uključuje, ali nije ograničen na, sljedeće:

- Gubitak ili krađu povjerljivih ili osjetljivih podataka ili opreme na kojoj su pohranjeni takvi podaci (npr. gubitak prijenosnog računala, USB stick, iPad/tablet uređaj ili papirnati zapis);
- Krađa ili neuspjeh opreme;
- Neovlaštena uporaba, pristup ili izmjena podataka ili informacijskih sustava;
- Pokušaji (neuspješni ili uspješni) neovlaštenog pristupa informacijama ili IT-u sustavu;
- Neovlašteno otkrivanje osjetljivih / povjerljivih podataka;
- Zlouporaba web stranica;
- Neočekivane okolnosti poput požara ili poplave;
- Ljudska pogreška;
- Kaznena djela u kojima se dobivaju informacije obmanom.

4. Otkrivanje povrede osobnih podataka

Voditelj će kontinuirano provoditi:

- tehnološke mjere za otkrivanje povrede osobnih podataka;
- organizacijske mjere za otkrivanje povrede osobnih podataka;
- redoviti pregled mjera za otkrivanje povrede osobnih podataka.

5. Prijavljivanje incidenta

- Svatko tko pristupa, koristi ili upravlja osobnim podacima i informacijama kod Voditelja, obvezan je o povredama podataka i incidenta sigurnosti informacija odmah obavijestiti:
  1. Povjerenika za zaštitu privatnosti:
     a) E-mail: maricveso@cki-m.com;
     b) Tel.: 01 2442 193
  2. Ravnatelja:
     a) E-mail: ravnatelj@cki-m-com;
     b) Tel.: 01 2442 193
- Ako se prekršaj dogodi ili se otkrije izvan redovnog radnog vremena, mora se prijaviti
- što je prije moguće.
- Izvješće će sadržavati potpune i točne podatke o incidentu, kada je došlo do povrede (datum i vrijeme), priroda povrede, Informacije o kategorijama podataka, vrstama podataka, koliko je osoba pogođeno i ostale važne informacije, sukladno ovom pravilniku.

6. Ograničenje i oporavak

- Povjerenik za zaštitu privatnosti (*nadalje **PZP***) prvo će utvrditi je jesu li povrede još uvijek u tijeku. Ako je tako, odmah će poduzeti odgovarajuće korake kako bi se smanjio učinak povreda.
- Početne odluke donosi PZP u suradnji s relevantnim osobama za utvrđivanje ozbiljnost povreda i utvrđuje tko će voditi istragu o povredama (to će ovisno o prirodi povreda u nekim slučajevima biti PZP).
- Voditelj istražnog tima će utvrditi postoji li nešto što se može učiniti kako bi vratili sve gubitke i ograničiti štetu koju bi mogle prouzročiti povrede.
- PZP će utvrditi tko može biti obaviješten kao i je li potrebno obavijestiti policiju, kad je to prikladno.
- Savjeti stručnjaka Voditelja mogu se tražiti u rješavanju incidenta.
- PZP u suradnji s nadležnim službenim osobljem, određuje odgovarajući tijek akcije koje treba poduzeti kako bi se osiguralo rješavanje incidenta.

7. Istraživanje i procjena rizika

Istraživanje će obaviti PZP odmah i gdje god je to moguće u roku od **24 sata** od otkrivanja/prijavljivanja prekršaja.

PZP će istražiti povrede i procijeniti rizike povezane s njima, na primjer, potencijalne štetne posljedice za pojedince, koliko su one ozbiljne ili značajne i koliko je vjerojatno da će se ponoviti.

Istraga će morati uzeti u obzir sljedeće:

- vrstu podataka koji su uključeni
- njihovu osjetljivost
- postoje li zaštitne mjere (npr. šifriranje)
- što se dogodilo s podacima, je li izgubljeno ili ukradeno
- mogu li podaci biti stavljeni na bilo kakvu ilegalnu ili neprikladnu uporabu

- koji su pojedinci, broj uključenih pojedinaca i potencijalni učinci povrede na osobne podatke tih pojedinaca
- postoje li šire posljedice povreda

8. Obavijest

PZP, u dogovoru s upravom Voditelja obrade, će odrediti tko treba biti obaviješten o povredi.

Svaki se incident ocjenjuje od slučaja do slučaja; međutim, sljedeće će trebati uzeti u obzir:

- Postoje li zakonski/ugovoreni zahtjevi za obavješćivanje;
- Hoće li obavijest pomoći pojedincima koji su pogođeni - bi li mogli djelovati na informacije za ublažavanje rizika?
- Hoće li obavijest pomoći u sprječavanju neovlaštenog ili nezakonitog korištenja osobnih podataka?
- Hoće li obavijest pomoći Voditelju da ispuniti svoje obveze prema srodnim podacima - načelo zaštite?
- Ako je pogođen velik broj ljudi ili postoje vrlo ozbiljne posljedice, treba li obavijestiti nadzorno tijelo -AZOP- podaci dostupni na njihovoj web stranici;
- Obavijest osobama na čije osobne podatke utječe incident, će uključiti opis kako i kada je došlo do kršenja i kojih podataka. Posebno se daju jasni savjeti o tome što mogu učiniti kako bi se zaštitili i obavijest što je već poduzeto za ublažavanje rizika. Pojedinci će također dobiti obavijest o načinu na koji mogu kontaktirati voditelja za daljnje informacije ili postavljati pitanja - što se dogodilo.
- PZP mora razmotriti obavještavanje trećih strana kao što su policija, osiguravatelji, banke ili Kreditno kartični odjeli i sindikate. To bi bilo prikladno tamo gdje je protuzakonita aktivnost poznata ili se vjeruje da je došlo ili gdje postoji rizik od pojave nezakonite aktivnosti u budućnosti.
- PZP će razmotriti treba li obavijestiti komunikacijski tim s obzirom na priopćenje za tisak i da budu spremni za obradu svih dolaznih press upita.
- Sve radnje će evidentirati PZP.

9. Procjena i odgovor

Nakon što je inicijalni incident zadržan, PZP će provesti cjeloviti pregled uzroka povreda; učinkovitost odgovora na povrede i utvrditi potrebu za bilo kakve promjene u sustavima i politikama i potrebu poduzimanja postupaka.

Postojeće mjere će biti pregledane kako bi se utvrdila njihova adekvatnost i treba li poduzeti neke ispravke ili akciju kako bi se smanjila opasnost od sličnih incidenata.

Pregled će razmotriti:

- Gdje se i kako drže osobni podaci i gdje i kako se pohranjuju;
- Gdje su najveći rizici i identificirat će sve daljnje potencijalne slabe točke unutar postojećih mjera;
- Jesu li metode prijenosa sigurne; je li potrebno smanjiti količinu dijeljenja podataka;
- Osvješćivanje osoblja;

- Provedba plana postupanja kod povrede podataka i utvrđivanje skupine odgovornih osoba odgovornih za reagiranje na prijavljene povrede sigurnosti;

Ako se smatra potrebnim, izvješće koje preporučuje bilo kakve promjene u sustavima, politikama i postupcima, će razmatrati uprava Voditelja.

10. Obavijest nadzornom tijelu (čl.33.GDPR) **(Obrazac 1.):**
Obrazac se primjenjuje kada voditelj obrade podataka ima obvezu obavijestiti nadzorno tijelo o povredi osobnih podataka. Obrazac sadrži: postupak za prijavu povrede osobnih podataka nadzornom tijelu; izuzetak od obveze obavještavanja nadzornog tijela o povredi osobnih podataka; dodatne informacije koje se dostavljaju nadzornom tijelu; promjene činjenica koje se odnose na povredu osobnih podataka i trebaju biti dostavljene nadzornom tijelu.

11. Obavijest voditelju obrade podataka (Obrazac 2.):
Obrazac se primjenjuje kada i ako voditelj obrade angažira tvrtku - izvršitelj obrade podataka ima obvezu obavijestiti voditelja podataka o povredi osobnih podataka. Obrazac sadrži: postupak za prijavu povrede osobnih podataka voditelju obrade podataka; dodatne informacije koje će se dati voditelju obrade podataka.

12.Obavijest ispitanicima – pojedincima (čl.34.GDPR) **(Obrazac 3.):**
Obrazac se primjenjuje kada Voditelj obrade podataka, obavješćuje ispitanika u dogovoru s nadzornim tijelom. Obrazac sadrži: postupak za prijavu povrede osobnih podataka ispitanicima; izuzetak od obveze obavještavanja ispitanika o kršenju osobnih podataka; diskrecijska obavijest o kršenju osobnih podataka ispitaniku.

13. Interna evidencija povreda (čl.34.st. 5. GDPR) **(Obrazac 4.):**
Obrazac se primjenjuje kako bi Voditelj obrade interno evidentirao povrede i poduzeo mjere. Obrazac sadrži: sve informacije o povredi koje su od utjecaja na obveze voditelja obrade.

14. Pregledavanje i ažuriranje ove politike:

- Osobe odgovorne za pregled i ažuriranje politike: Uprava društva i Službenik za zaštitu osobnih podataka
- Godišnji pregled politike: obvezno jednom godišnje.
- „Ad hoc“ preispitivanje politike: u svakom slučaju kada se sumnja u slabosti politike.
- Pitanja koja treba uzeti u obzir prilikom preispitivanja politike: sva pitanja koja su od utjecaja na prvinu primjenu odredbi GDPR, posebice kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:
    a) pseudonimizaciju i enkripciju osobnih podataka;
    b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
    c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
    d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Sastavni dio ovog pravilnika su prilozi (obrasci br.1.-4.)
Ovaj Pravilnik biti će objavljen na oglasnoj ploči Voditelja obrade.
Ovaj Pravilnik stupa na snagu protekom osmog dana od dana objave.

U Zagrebu, 10. listopada 2018.

Za voditelja obrade:
Predsjednica Upravnog vijeća:

Zdenka Ninić

Obrazac 1
(Obavijest o kršenju osobnih podataka -nadzornom tijelu)
(čl.33. GDPR)

Nadzorno tijelo	Agencija za zaštitu osobnih podataka Martićeva ulica 14 HR - 10 000 Zagreb Tel. 00385 (0)1 4609-000 Fax. 00385 (0)1 4609-099 E-mail: azop@azop.hr Web: www.azop.hr
Uvod: identifikacija osobe koja daje obavijest o povredi osobnih podataka. (Ime i prezime, kontakt podaci E-mail; tel.)	
Predstavljanje povrede osobnih podataka: Opći opis – priroda povrede osobnih podataka. Dokazi (dokumenti):	
Kategorije ispitanika koje su pogođene i približan broj dotičnih ispitanika	
Približan broj dotičnih evidencija podataka koji su pogođeni.	
Broj pogođenih podataka:	
Kategorije osobnih podataka kojih se tiču.	
Broj podataka o kojima je riječ:	
Vjerojatne posljedice povrede:	
Mjere koje se poduzimaju radi rješavanja problema povreda: Dokazi (dokumenti):	
Mjere koje su poduzete za umanjivanja mogućih štetnih posljedica povrede osobnih podataka. Dokazi (dokumenti):	
Je li povreda prijavljena ispitanicima?	
Kašnjenje izvješća o povredi? Razlozi za kasno izvješće o kršenju osobnih podataka:	
Priložena dokumentacija	
Pojedinosti o kontakt osobi: (Ime i prezime, kontakt podaci E-mail; tel.)	

**U slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvješćuje nadzorno tijelo nadležno u skladu s člankom 55. o povredi osobnih podataka, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje.*
**Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane za povredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete. Ta dokumentacija nadzornom tijelu omogućuje provjeru poštivanja odredbi (Članak 33. GDPR)*

Obrazac 2
(Obavijest o kršenju osobnih podataka- voditelju obrade podataka)

(Čl. 33.st.2. GDPR)

Uvod: identifikacija osobe koja daje obavijest o povredi osobnih podataka. (Ime i prezime, kontakt podaci E-mail; tel.)	
Predstavljanje povrede osobnih podataka: Opći opis – priroda povrede osobnih podataka. Dokazi (dokumenti).	
Kategorije ispitanika koje su pogođene i približan broj dotičnih ispitanika.	
Približan broj dotičnih evidencija podataka koji su pogođeni.	
Broj pogođenih podataka.	
Kategorije osobnih podataka kojih se tiču.	
Broj podataka o kojima je riječ.	
Vjerojatne posljedice povrede:	
Mjere koje su poduzete za umanjivanja mogućih štetnih posljedica povrede osobnih podataka. Dokazi (dokumenti)	
Priložena dokumentacija.	
Pojedinosti o kontakt osobi: (Ime i prezime, kontakt podaci E-mail; tel.)	

Obrazac 3
(Obavijest o kršenju osobnih podataka -ispitaniku)
(Čl.34.GDPR)

Uvod: identifikacija osobe koja daje obavijest o povredi osobnih podataka. (Ime i prezime, kontakt podaci E-mail; tel.)	
Predstavljanje povrede osobnih podataka: Opći opis – priroda povrede osobnih podataka.	
Kategorije osobnih podataka koji su povrijeđeni.	
Vjerojatne posljedice povrede:	
Mjere koje se poduzimaju radi rješavanja problema povreda:	
Mjere koje su poduzete za umanjivanja mogućih štetnih posljedica povrede osobnih podataka	
Obavješćivanje nije obvezno iz razloga: Ispunjen bilo koji od sljedećih uvjeta: *(a) voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;* *(b) voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz stavka 1.;* *(c) time bi se zahtijevao nerazmjeran napor. U takvom slučaju mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.*	
Priložena dokumentacija	
Pojedinosti o kontakt osobi: (Ime i prezime, kontakt podaci E-mail; tel.)	

** U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.(Članak 34. GDPR).*
Ova obavijesti nije obvezna , ako su osobni podaci pod enkripcijom ili ako su poduzete naknadne mjere koje otklanjaju visoki rizik ili ako bi obavješćivanje iziskivalo nerazmjeran napor voditelj obrade i izvršeno je javno obavješćivanje ili slična mjera.

Obrazac 4.
Interna obavijest o povredi osobnih podataka
(Čl.33.st.5. GDPR)

Ime osobe za izvješćivanje: Kontakt za daljnje informacije što se tiče incidenta: (Ime i prezime, kontakt podaci E-mail; tel.)	
Mjesto i datum davanja obavijesti:	
Datum i vrijeme (ako je poznato) incidenta	
Mjesto incidenta	
Okolnosti/opis incidenta	
Vrstu podataka koji su povredom izloženi riziku	
Koliko je to osjetljivo? * Neki su podaci osjetljivi zbog svoje osobne prirode (npr. podaci o zdravlju) dok su druge vrste podataka osjetljivi zbog onoga što bi se moglo dogoditi ako su zloupotrijebljena (npr. podaci o bankovnom računu).	
Može li povreda? a) staviti u opasnosti bilo kakve podatke (rizik za zdravlje)? b) dovesti do krađe identiteta? c) učiniti d privatni život osobe bude poznat drugima, npr. Financijska okolnosti?	
Broj ispitanika i određene kategorije podataka koji su pogođeni?	
Kako su osoblje postalo svjesno incidenta?	
Je li netko od ispitanika svjestan toga da se dogodio incident? Ako je tako, koliko?	
Jeste li poduzeli bilo kakvu akciju? (kako bi minimizirali/ublažili učinak na podatke). Ako jeste, navedite detalje. Koji su subjekti uključeni.	
Je li pokrenuta unutarnja istraga? Ako je tako, navedite pojedinosti.	
Jeste li upoznali neko drugo regulatorno tijelo s materijom? Ako jeste, molimo navedite detalje.	
Koje ćete radnje poduzeti kako biste spriječili slične incidente u budućnosti?	
Navedite sve ostale informacije koje biste smatrali korisnima.	