GDPR - Opća uredba o zašiti osobnih podataka

Muzej – Museo Lapidarium, Veliki trg 8a, Novigrad - Cittanova

ANALIZA USKLAĐENOSTI POSLOVANJA S OPĆOM UREDBOM O ZAŠTITI OSOBNIH PODATAKA

Voditelj analize:

Istra GDPR d.o.o.
Armando Ujčić
službenik za zaštitu podataka

1. Sažetak

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) (u daljnjem tekstu: Uredba) je stupila na snagu 24. svibnja 2016., a postala je izravno primjenjiva u svim državama članicama Europske Unije 25. svibnja 2018.

Uredba zamjenjuje stari Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12) koji je prestao važiti 25. svibnja 2018. i njegove podzakonske akte, a novi pravni okvir čine Uredba, Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) te postojeći posebni zakoni.

Polazišna točka i temelj svega jest da svatko ima pravo na zaštitu svojih osobnih podataka. Uredba bi trebala građanima pružiti veću kontrolu nad njihovim osobnim podacima, a s druge strane poslovnim subjektima i javnim tijelima nametnuti obvezu odgovornog korištenja osobnih podataka građana.

U ovoj analizi su dani kratki parametri u smjeru poznavanja i razumijevanja Uredbe, te su spomenuta najvažnija načela i pojmovi važni za razumijevanje Uredbe.

Svrha analiziranja obrade osobnih podataka je utvrđivanje usklađenosti obrade osobnih podataka s Općom uredbom o zaštiti osobnih podataka, odnosno davanje preporuke i izrađivanje potrebnih pravnih akata potrebnih za usklađenje s Uredbom.

Opisuje se način provođenja postupka implementacije Uredbe te se pristupa analizi postojećeg stanja koje se sastoji od informatičkog sustava, video nadzora, pravnog sustava te organizacijskih i tehničkih mjera. Konačno, u sklopu ove analize su dane pravne i informatičke preporuke u odnosu na analizirano stanje, posebno za svaku od navedenih stavaka, a naposljetku se nalazi i kratki tablični prikaz.

2. Sadržaj

3. Uvod

Muzej – Museo Lapidarium (u daljnjem tekstu: Muzej) je javna ustanova za obavljanje muzejske djelatnosti kao javne službe. Sjedište muzeja je u Novigradu, Veliki trg 8a.

U sklopu iskazane potrebe za usklađenjem poslovanja Muzej-a s Uredbom, djelatnici istog su pristupili edukaciji i usklađenju pravnih akata s Uredbom.

Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo. Svatko ima pravo na zaštitu svojih osobnih podataka.

Uredba je stupila na snagu 24. svibnja 2016., međutim ista postaje izravno primjenjiva u svim državama članicama Europske Unije tek 25. svibnja 2018., čime je državama članicama dano prijelazno razdoblje prilagodbe.

Uredba zamjenjuje stari Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12) koji je prestao važiti 25. svibnja 2018. i njegove podzakonske akte, a novi pravni okvir čine Uredba, Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) te postojeći posebni zakoni.

Polazišna točka i temelj svega jest da svatko ima pravo na zaštitu svojih osobnih podataka. Uredba bi trebala građanima pružiti veću kontrolu nad njihovim osobnim podacima, a s druge strane poslovnim subjektima i javnim tijelima nametnuti obvezu odgovornog korištenja osobnih podataka građana.

Gospodarska i društvena integracija proizašla iz funkcioniranja unutarnjeg tržišta dovela je do znatnog povećanja prekograničnih protoka osobnih podataka. Povećala se razmjena osobnih podataka između javnih i privatnih sudionika, uključujući pojedince, udruženja i poduzetnike širom Europske Unije. Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti osobnih podataka. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje uporaba osobnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno.

Za takav razvoj potreban je čvrst i usklađeniji okvir za zaštitu podataka u Uniji koji se temelji na odlučnoj provedbi s obzirom na važnost stvaranja povjerenja koje će omogućiti razvoj digitalne ekonomije na čitavom unutarnjem tržištu. Pojedinci bi trebali imati nadzor nad vlastitim osobnim podacima.

Kako bi se osigurala dosljedna razina zaštite pojedinaca širom Unije i spriječila razilaženja koja ometaju slobodno kretanje osobnih podataka na unutarnjem tržištu, potrebna je Uredba radi pružanja pravne sigurnosti i transparentnosti gospodarskim subjektima, uključujući mikropoduzeća, mala i srednja poduzeća, te pružanja pojedincima u svim državama članicama istu razinu pravno primjenjivih prava i obveza te odgovornosti za voditelje obrade i izvršitelje obrade kako bi se osiguralo postojano praćenje obrade osobnih podataka i jednake sankcije u svim državama članicama, kao i djelotvornu suradnju između nadzornih tijela različitih država članica. Za ispravno funkcioniranje unutarnjeg tržišta ne ograničava se niti zabranjuje slobodno kretanje osobnih podataka u

Uniji zbog razloga povezanih sa zaštitom pojedinaca u vezi s obradom osobnih podataka. Ova Uredba sadržava odstupanja za organizacije u kojima je zaposleno manje od 250 osoba s obzirom na vođenje evidencije, radi uzimanja u obzir posebnih situacija mikropoduzeća, malih i srednjih poduzeća. Osim toga, institucije i tijela Unije te države članice i njihova nadzorna tijela potiču se da u primjeni ove Uredbe uzmu u obzir posebne potrebe mikropoduzeća, malih i srednjih poduzeća.

Zaštita koja se pruža ovom Uredbom u vezi s obradom osobnih podataka trebala bi se odnositi na pojedince bez obzira na njihovu nacionalnost ili boravište. Ovom se Uredbom ne obuhvaća obrada osobnih podataka koji se tiču pravnih osoba, a osobito poduzetnika koji su ustanovljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe.

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.

Cilj ove GAP analize je dati preporuke i izraditi sve potrebne pravne akte potrebne za usklađenje s Općom uredbom o zaštiti osobnih podataka.

3.1. Pojmovi, načela, obveze i prava sudionika obrade osobnih podataka

Sukladno Uredbi, osobni podatak je svaki podatak koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi. Obrada je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima. Dakle, obrada obuhvaća apsolutno sve radnje s osobnim podacima, 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.

Načela zaštite podataka trebala bi se primjenjivati na sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Kako bi se odredilo može li se identitet pojedinca utvrditi, trebalo bi uzeti u obzir sva sredstva, poput primjerice selekcije, koja voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj. Načela zaštite podataka stoga se ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili

se može utvrditi ili na osobne podatke koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi. Ova se Uredba stoga ne odnosi na obradu takvih anonimnih informacija, među ostalim za statističke ili istraživačke svrhe.

Privola bi se trebala davati jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave. To bi moglo obuhvaćati označivanje polja kvačicom pri posjetu internetskim stranicama, biranje tehničkih postavaka usluga informacijskog društva ili drugu izjavu ili ponašanje koje jasno pokazuje u tom kontekstu da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom. Privola bi trebala obuhvatiti sve aktivnosti obrade koje se obavljaju u istu svrhu ili svrhe. Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih. Ako se privola ispitanika treba dati nakon zahtjeva upućenog elektroničkim putem, taj zahtjev mora biti jasan, jezgrovit i ne smije nepotrebno ometati upotrebu usluge za koju se upotrebljava.

Načela i pravila o zaštiti pojedinaca u vezi s obradom njihovih osobnih podataka trebala bi poštovati njihova temeljna prava i slobode, a posebno njihovo pravo na zaštitu osobnih podataka, bez obzira na nacionalnost ili boravište pojedinaca. Ovom Uredbom želi se doprinijeti uspostavi područja slobode, sigurnosti i pravde te gospodarske unije, gospodarskom i socijalnom napretku, jačanju i približavanju gospodarstava na unutarnjem tržištu te dobrobiti pojedinaca.

Svaka obrada osobnih podataka trebala bi biti zakonita i poštena. Za pojedince bi trebalo biti transparentno kako se osobni podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti osobni podaci obrađuju ili će se obrađivati. Načelom transparentnosti traži se da svaka informacija i komunikacija u vezi s obradom tih osobnih podataka bude lako dostupna i razumljiva te da se upotrebljava jasan i jednostavan jezik. To se načelo osobito odnosi na informacije ispitaniku o identitetu voditelja obrade i svrhama obrade te daljnje informacije radi osiguravanja poštenosti i transparentnosti obrade s obzirom na pojedince o kojima je riječ i njihovo pravo da dobiju potvrdu i na obavijest o osobnim podacima koji se obrađuju, a koji se odnose na njih. Osobito, određena svrha u koju se osobni podaci obrađuju trebala bi biti izrijekom navedena i opravdana te određena u vrijeme prikupljanja osobnih podataka. Osobni podaci trebali bi biti primjereni, bitni i ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju. Zbog toga je osobito potrebno osigurati da je razdoblje u kojem se osobni podaci pohranjuju ograničeno na strogi minimum. Osobni podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima. Radi osiguravanja da se osobni podaci ne drže duže nego što je nužno, voditelj obrade trebao bi odrediti rok za brisanje ili periodično preispitivanje. Trebalo bi poduzeti svaki razumno opravdani korak radi osiguravanja da se netočni osobni podaci isprave ili izbrišu. Osobne podatke trebalo bi obrađivati uz odgovarajuće poštovanje sigurnosti i povjerljivosti osobnih podataka, što obuhvaća i sprečavanje neovlaštenog pristupa osobnim podacima i opremi kojom se koristi pri obradi podataka ili njihove neovlaštene upotrebe.

Dakle, Uredba nalaže da obrada osobnih podataka mora biti u skladu s nekim pravnim temeljem, a načelima poštenosti i transparentnosti se zahtijeva da je ispitanik informiran o postupku obrade i njegovim svrhama, dok je voditelj obrade dužan ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade, uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka.

Zakoniti pravni temelji obrade osobnih podataka su:

- zakonska obveza voditelja obrade,

- nužnost izvršenja ugovora,

- privola ispitanika,

- zaštita interesa ispitanika/druge osobe,

- zaštita javnog interesa/izvršenje službenih ovlasti, i

- legitimni interes voditelja obrade.

Nadalje, sukladno načelu ograničavanja svrhe, osobni podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se ne smiju obrađivati na način koji nije u skladu s tim svrhama. Dakle, podaci koji su pribavljeni moraju se koristiti samo u svrhe na koje je pojedinac pristao. Moguća je daljnja obrada samo u slučajevima koji su u javnom interesu ili u svrhu znanstvenog ili povijesnog istraživanja te u statističke svrhe.

Načelo smanjenja količine podataka je jedno o najbitnijih načela i zahtjeva Uredbe. Ono kazuje kako osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju. Dakle, podaci mogu biti obrađeni samo za onu svrhu zbog koje su prikupljeni i kojoj su namijenjeni. Na to se nadovezuje načelo ograničenja pohrane sukladno kojem osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Dakle, pribavljeni podaci mogu biti čuvani koliko je potrebno za određenu obradu, a duže mogu biti pohranjeni jedino u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesno istraživanja ili u statističke svrhe, što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih Uredbom radi zaštite prava i sloboda ispitanika.

Načelo pouzdanosti objedinjuje sva načela te nameće voditelju obrade odgovornost za usklađenost s načelima obrade osobnih podataka kao i za mogućnost dokazivanja usklađenosti. Dakle, podloga za organizacijske zahtjeve koje nameće Uredba jest temeljna odgovornost za usklađenost koja u osnovi sadrži dva elementa: osigurati usklađenost s uredbom i biti sposoban dokazati usklađenost s Uredbom.

Ispitanik bi trebao imati pravo na ispravak osobnih podataka koji se na njega odnose te „pravo na zaborav" ako zadržavanje takvih podataka krši ovu Uredbu ili pravo Unije ili pravo države članice koje se primjenjuje na voditelja obrade. Ispitanici bi osobito trebali imati pravo da se njihovi osobni podaci brišu i više ne obrađuju ako ti osobni podaci više nisu potrebni s obzirom na svrhu u koju su prikupljeni ili na druge načine obrađivani, ako su ispitanici povukli svoju privolu ili ako daju prigovor na obradu osobnih podataka koji se

odnose na njih ili ako obrada njihovih osobnih podataka na druge načine nije u skladu s ovom Uredbom. Ovo je pravo osobito bitno ako je ispitanik dao svoju privolu dok je bio dijete i nije bio u potpunosti svjestan rizika obrade, a kasnije želi ukloniti takve osobne podatke, osobito na internetu. Ispitanik bi trebao biti u mogućnosti ostvariti to pravo neovisno o činjenici da više nije dijete. No daljnja pohrana osobnih podataka trebala bi biti zakonita ako je nužna za ostvarivanje prava na slobodu izražavanja i na slobodu informiranja, radi poštovanja pravnih obveza, za izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade, na temelju javnog interesa u području javnog zdravlja, u svrhe arhiviranja od javnog interesa, u svrhe znanstvenih ili povijesnih istraživanja, u statističke svrhe ili za postavljanje, ostvarivanje ili obranu pravnih zahtjeva.

Konačno, Uredba nije apsolutno pravo, već pravo koje se treba balansirati s drugim pravima koji su definirani unutar neke države. Obrada osobnih podataka trebala bi biti osmišljena tako da bude u službi čovječanstva. Pravo na zaštitu osobnih podataka nije apsolutno pravo, što znači da ga se mora razmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti.

Cilj ove GAP analize je utvrditi postojeće stanje, dati informatičke i pravne preporuke i izraditi sve potrebne pravne akte potrebne za usklađenje s Općom uredbom o zaštiti osobnih podataka.

4. Način rada

Odgovorne osobe i djelatnici Muzeja sudjelovali su na provedenim edukacijama o zašiti i usklađenju s Općom uredbom o zaštiti osobnih podataka. Sastavni dio edukacije je i prikupljanje podataka o trenutnom stanju i usklađenosti s GDPR direktivom. Putem ispunjenih upitnika Muzeja dobiveni su osnovni podaci o trenutnom stanju u ustanovi. Upitnici su dani i popunjavani u pisanom obliku.

Muzej je ispunio upitnik A. Evidencija aktivnosti obrade i Upitnik B. Načela i principi rada. Na osnovi tih ispunjenih upitnika i obrade rezultata napravljena je analiza. Rezultati ove analize su potrebni dokumentni i preporuke za usklađenje s Uredbom.

Odgovorne osobe u Muzeju prošle su uvodnu i završnu edukaciju u kojoj su upoznate s osnovnim pojmovima iz Uredbe, načelima, pravima i obvezama sudionika obrade osobnih podataka, kao i ciljevima same Uredbe te konkretnim primjerima iz stvarnog života i poslovnog svijeta. Također, obavljeni su razgovori s odgovornim osobama te je izvršen uvid u javno dostupne podatke.

5. Analiza postojećeg stanja

5.1. IT- informatički sustav

Muzej posjeduje vlastiti serverski sustav na koji je spojena lokalna računarska mreža.

U cilju zaštite podataka i njihovog čuvanja redovito se radi kopiranje podataka na vanjsku memorijsku jedinicu.

Server računarskog sustava nalazi se u uredu koji je van radnog vremena zaključan i nije dostupan.

Sva su računala nisu zaštićena korisničkim imenom i lozinkom.

Muzej ne posjeduje sustav koji evidentira pristup podacima. Ne posjeduju elektronički sustav evidencije radnog vremena kao niti elektronički sustav pristupa, Muzej ne posjeduje sustav bilježenja neovlaštenih pokušaja pristupa podacima.

Evidencije koje se pohranjuju digitalno, pohranjuju se na osobnim računalima zaposlenika i serveru računarskog sustava.

Pristup javnoj internetskoj mreži je slobodan i besplatan za sve zaposlenike. Ne ograničava se pristup javnim servisima i društvenim mrežama.

Na osobnim računalima pristupne lozinke ne mijenjaju se redovito. Sva računala zaštićena su antivirusnim programima i programima za zaštitu od krađe podataka ili zlonamjernog korištenja.

Tvrtka ne posjeduje standardizirane procedure informatičke sigurnosti.

Određene informatičke usluge za tvrtku obavljaju vanjski suradnici ili vanjske tvrtke.

Muzej ima ugovor o informatičkom održavanju s vanjskom tvrtkom. Vanjska tvrtka koje obavlja informatičke usluge ima pristup određenim podacima informatičkog sustava.

Računovodstvene usluge obavlja vanjski računovodstveni servis. Računovodstveni servis nema pristup svim potrebnim podacima zapisanim u digitalnom obliku a koji se nalaze na serveru sustava ili na osobnim računalima zaposlenika.

5.2. Video nadzor

Muzej posjeduje vlastiti sustav video nadzora. Muzej ima mogućnost uvida u video zapise te informacije o načinu i ovlaštenim osobama za pregledavanja video zapisa te vodi brigu o čuvanju video zapisa.

5.3. Pravni sustav

U sklopu provođenja implementacije Uredbe i postupka usklađivanja, Muzej je poduzeo sljedeće korake:

- održana je edukacija predstavnika Muzeja na temu implementacije i primjene Uredbe u svakodnevnom poslovanju

- donesena je i objavljena Odluka o imenovanju službenika za zaštitu podataka, čime je ispunjen uvjet objave kontakt podataka službenika za zaštitu podataka, a Izvješće o imenovanju službenika za zaštitu podataka je pravovremeno dostavljeno nadzornom tijelu, Agenciji za zaštitu osobnih podataka,

- izrađene su Izjave o povjerljivosti kojima potpisnik pod punom materijalnom i radnopravnom odgovornošću izjavljuje da je upoznat s primjenom Uredbe te da će za vrijeme trajanja zaposlenja, a i nakon prestanka, postupati odgovorno sa svim osobnim podacima do kojih dođe u sklopu obavljanja svojih radnih dužnosti. Izjave su dane na potpis svim zaposlenicima Muzeja,

- Izjava o zaštiti privatnosti je objavljena na službenoj internetskoj stranici Muzeja, čime su ispitanici upoznati sa svojim osnovnim pravima,

- donesen je te Pravilnik o prikupljanju, obradi, korištenju i zaštiti osobnih podataka. Isti je objavljen na internetskoj stranici,

- ne postoji Pravilnik o korištenju elektroničke pošte i drugih oblika komunikacije,

- nije izrađen i sklopljen Sporazum o obradi podataka s izvršiteljima obrade,

- izrađeni su nacrti izjava ispitanika kojom isti daju privolu odnosno odustaju od dane privole za obradu njihovih osobnih podataka.

- formirana je evidencija aktivnosti obrade sa sljedećim sustavima pohrane: evidencija o radnicima, dosje radnika, evidencija radnog vremena, prijave na natječaj za zapošljavanje, poslovni partneri, projektni partneri, vanjski suradnici na projektu, popis kontakata sudionika radionica, predavanja, konferencija, liste dionika, kontrolna tijela.

5.4. Organizacijske i tehničke mjere

Primjena Uredbe obuhvaća kako digitalizirani oblik obrade i pohrane osobnih podataka, tako i materijalizirani, odnosno prikupljanje, obradu i pohranjivanje osobnih podataka u fizičkom obliku. Iz tog razloga je bitno poduzeti određene organizacijske i tehničke mjere kako bi se rizik povrede osobnih podataka sveo na minimum.

Muzej čuva osobne podatke u materijalnom (fizičkom) i u digitalnom obliku. Osobni podaci koji se obrađuju u sklopu djelovanja Muzeja su pohranjeni u uredu koji se nakon radnog vremena zaključava. Papirnata dokumentacija čuva se u ormarima pod ključem. Elektronska dokumentacija nalazi se na računalima i serveru koji nisu zaštićeni lozinkom.

6. Preporuke

6.1. IT- informatički sustav

6.1.1. Pristup podacima

Dodjela pristupnih prava korisnika provodi se s ciljem omogućavanja ispravnog korištenja programa, podataka.

Sistem administrator je ovlaštena osoba od tvrtke Muzeja za administriranje i upravljanje računarskim sustavom, svim njegovim sastavnicama. Sistem administrator može biti zaposlenik tvrtke ili ovlaštena osoba vanjske IT tvrtke s kojom postoji ugovor o informatičkom održavanju.

Radi provođenja mjere dodjele pristupnih prava korisnicima mreže, aplikacija i baza podataka pohranjenih u računalima, preporuka je provoditi sljedeće radnje:

- Sistem administrator, dužan je omogućiti uređaje i softver za autentifikaciju korisnika koji pristupaju računarskom sustavu,
- Sistem administrator dužan je organizirati pristup i provesti kontrolu pristupa svim računalnim sustavima samo ovlaštenim djelatnicima primjereno zahtjevima posla kojeg obavljaju,
- Sistem administrator dužan je provesti sve nadopune, brisanja i promjene u organizaciji i kontroli pristupa računalnim sustavima u skladu s odobrenim zahtjevom krajnjeg korisnika,
- Sistem administrator dužan je onemogućiti anonimni pristup bilo koje vrste do radnih stanica,
- Sistem administrator dužan je kontrolirati modemske i slične priključke na mrežu, a instalaciju novih modema, usmjerivača i ostale mrežne opreme odobrava sistem administrator,
- Sistem administrator dužan je pratiti sva događanja na mreži,
- Korisnik računalnog sustava je odgovoran za sve računalne transakcije izvršene uz uporabu njegove korisničke identifikacije i lozinke (korisničkog računa),
- Lozinka se mora mijenjati u roku ne dužem od godine dana, a obveza voditelja obrade je upozoriti svoje djelatnike na potrebu redovitog mijenjanja lozinki,
- Ne smiju se koristiti lozinke koje se mogu lako pamtiti i lako odgonetnuti ili probiti od strane drugih osoba niti se ista lozinka može upotrebljavati dva puta zaredom,
- Lozinke moraju sadržavati najmanje pet znakova i to kombinaciju slova, brojki i simbola,

• Korisnik mora odjaviti svoj korisnički račun kada prestaje s radom na računalu na duže vrijeme,

• Osoba zadužena za kadrovske evidencije dužna je promptno obavijestiti Sistem administratora o tome da li nekom djelatniku prestaje radni odnos ili se raspoređuje na rad na drugo radno mjesto, kako bi se mogla regulirati njegova ovlaštenja za pristup resursima odnosno ukinuti korisnički račun,

• Radna stanica može se ugasiti kada nije u upotrebi (npr. preko noći), Ukoliko je neophodno za rad na daljinu korisnik svoju radnu stanicu može ostaviti uključenu.

6.1.2. Održavanje sustava od strane drugih pravnih osoba

Održavanje sustava od strane drugih pravnih osoba provodi se uz odobrenje Muzeja.

Zaposleni u pravnim osobama koji obavljaju određene poslove za Muzej za vrijeme obavljanja tih poslova, dužni su provoditi mjere zaštite sigurnosti.

Sistem administrator dužan je upoznati sve gore navedene osobe s mjerama zaštite i sigurnosti informatičkog sustava Muzeja.

6.1.3. Pristup internetu i elektronička pošta

Sigurno korištenje Interneta i elektroničke pošte provodi se u cilju sprječavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprječavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Tajnost elektroničke komunikacije ne može uvijek biti osigurana. Ona može biti kompromitirana zbog primjenjivosti zakona ili politike, nenamjernom distribucijom ili zbog neadekvatnosti postojećih tehnologija za zaštitu od neovlaštenog pristupa. Stoga se zaposlenici upućuju na povećani oprez kada se koriste bilo kojom vrstom elektroničke komunikacije.

Radi sigurnog korištenja Interneta i elektroničke pošte preporuka je provoditi sljedeće radnje:

• odgovaranje na e-poštu neka se odvija u što kraćem roku;

• poruke neka budu kratke i profesionalne;

• predmet poruke neka bude jasan i jednoznačan;

• treba izbjegavati slanje osobnih i povjerljivih informacija;

• treba izbjegavati raspravljati o osobnim stvarima preko adrese službene e-pošte;

• zabranjeno je slanje neželjene pošte (SPAM, CHAIN LETTER);

• izbjegavati opciju „Odgovori svima" ukoliko nije stvarno potrebna;

• izbjegavati slanje privitaka e-pošte većih od 5 MB ukoliko nije potrebno (za unutrašnju komunikaciju koristiti dijeljene mape na računalima);

• redovito arhivirati staru, ali važnu, e-poštu;

• antivirusna zaštita mora biti obavezno aktivirana kod primanja elektroničke pošte i pridruženih datoteka;

• zabranjeno je pokretanje sumnjivih izvršnih datoteka i onih iz nepouzdanih izvora.

6.1.4. Zaštita podataka

Zaštita podataka provodi se u cilju sprječavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprječavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja zaštite podataka potrebno je provoditi sljedeće radnje:

• Tvrdi disk (HDD-hard disk) s tajnim podacima moraju se pohranjivati pod ključem,

• Tvrdi disk treba pohranjivati na mjestima na kojima nisu izloženi vanjskim rizicima, kao što su toplina, izravna sunčeva svjetlost i magnetska polja,

• Sistem administrator je dužan osigurati, tamo gdje je potrebno, stvaranje sigurnosnih kopija podataka na magnetni/USB medij, mrežno dijeljene mape, SAN (Storage Area Network) ili Cloud (pohrana u oblaku) tehnologije, ovisno o raspoloživosti resursa,

Muzej redovito provodi kopiranje i sinkronizaciju podataka s lokalnih računala vanjsku memorijsku jedinicu. Preporučuje se da se tvrdi disk ili neki drugi medij na koji se vrši kopiranje nakon kopiranja čuva na mjestu koje je fizički udaljeno ili posebno zaštićeno.

Knjiga standarda informatičke sigurnosti nije obavezna, ona proizlazi iz ISO 27001 standarda. Nije obavezna ali je bezgranično korisna. Zaštita podataka je dinamičan proces, zbog same tematike kojom se bavi te i zbog promjena i novih načina pristupa i korištenja informatike. Samim time ne postoje trajno definirane procedure zaštite podataka već se one moraju stalno nadograđivati i pratiti promjene na polju zaštite podataka. To je jedan od glavnih razloga zbog kojih nisu propisani standardi informatičke sigurnosti već se oni kroz auditing ISO standarda nadograđuju i usklađuju. U tom smislu, iako nije obvezno, bilo bi korisno izraditi knjigu standarda informatičke sigurnosti.

6.1.5. Korištenje računalnih programa

Sigurno korištenje softvera provodi se u cilju sprječavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprječavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja zaštite softvera potrebno je provoditi sljedeće radnje:

- pridržavati se odredbi Zakona o autorskom pravu i srodnim pravima,
- pridržavati se licenčnih ugovora o korištenju autorski zaštićenog softvera,
- Sistem administrator je dužan voditi evidenciju o svim licencama softvera u posjedu Muzeja,
- Sistem administrator je dužan periodično, a najmanje jednom godišnje, izvršiti uvid u računala u posjedu tvrtke kako bi verificirao da je instaliran samo softver za čije korištenje tvrtka ima ovlaštenja,
- samo licencirani softver i softver u vlasništvu Muzeja smije se instalirati na računalima Muzeja,
- zabranjena je instalacija bilo kakvog softvera bez dozvole Sistem administratora,
- zabranjena je izmjena bilo kakvog softvera bez dozvole Sistem administratora,
- zabranjena je deinstalacija bilo kojeg softvera instaliranog na računalu bez dozvole Sistem administratora,

6.2. Video nadzor

Muzej ima potrebu donošenja pravilnika o provođenju videonadzora u skladu s Općom uredbom o zaštiti osobnih podataka.

6.3. Pravni sustav

Prava i obveze u odnosu na zaštitu osobnih podataka su, osim Uredbom i posebnim zakonima, uređeni i Pravilnikom o prikupljanju, obradi, korištenju i zaštiti osobnih podataka, Politikom privatnosti zaštite osobnih podataka i drugim aktima Muzeja čije se odredbe eventualno odnose na osobne podatke.

Sukladno članku 37. Uredbe, Muzej je obvezan, kao javnopravno tijelo, imenovati službenika za zaštitu podataka. Obveze imenovanog službenika za zaštitu podataka su

informiranje i savjetovanje voditelja obrade o obvezama iz područja zaštite podataka, praćenje poštivanja propisa o zaštiti podataka, suradnja s nadzornim tijelom, komunikacija s ispitanicima te posredovanje između ispitanika i voditelja obrade u svrhu poštivanja njihovih prava i pružanja kvalitetne zaštite tih prava. Slijedom navedenoga, a obzirom na propisane obveze, preporučujemo da imenovani službenik za zaštitu podataka redovito prati buduće promjene propisa, sudsku i upravnu praksu, kao i mišljenja Agencije za zaštitu podataka, te u skladu s time konstantno preispituje zakonitost obrade osobnih podataka u Muzeju. Ukoliko se utvrdi ikakva nepravilnost, potrebno je na to upozoriti odgovorne osobe i poduzeti potrebne mjere kako bi se nepravilnost uklonila.'

U odnosu na Izjavu o povjerljivosti, nakon što svi zaposlenici potpišu istu, preporučujemo ju uložiti u dosje zaposlenika.

Dostavljene obrasce Sporazuma o obradi podataka je potrebno ispuniti odgovarajućim podacima te iste sklopiti sa svim izvršiteljima obrade, onima koju obrađuju podatke u ime i po uputama Muzeja.

U sklopu implementacije Uredbe potrebno je regulirati postojeće i nove ugovorne odnose u svakodnevnom i redovnom poslovanju u odnosu na zaštitu osobnih podataka. Nije nužno odmah aneksirati i korigirati svaki sklopljeni ugovor, već je potrebno posebno obratiti pozornost na one ugovore temeljem kojih se izmjenjuje veći broj osobnih podataka, a ostale ugovore je moguće korigirati u hodu sukladno s ostalim obvezama iz konkretnog ugovora.[8]

Konačno, Upitnik A koji je ispunjen u svrhu provedbe GAP analize je sastavljen na način da isti može poslužiti kao evidencija aktivnosti obrade koju svakako preporučujemo voditi. To je dokument kojeg će Agencija tražiti na uvid u slučaju nadzora. Preporučujemo korigirati trenutno izrađene evidencije aktivnosti obrade na način da se istom obuhvate samo osobni podaci ispitanika na koje se primjenjuje Uredba. Naime, Uredba se ne primjenjuje na pravne osobe, kao niti na obrtnike i osobe koje se bave slobodnim zanimanjima, u onom opsegu koja je vezana za njihovu poslovnu djelatnost. Dakle, Uredba štiti fizičke osobe i njihovu privatnost. U tom smislu, preporučujemo korigirati evidenciju aktivnosti obrade (Upitnik A) na način da se izbace sve kategorije ispitanika i osobnih podataka koje nisu obuhvaćene poljem primjene Uredbe. Jednom kada je ta evidencija sastavljena, potrebno ju je pratiti te redovno dopunjavati i korigirati u slučaju eventualnih promjena u poslovanju.

6.4. Organizacijske i tehničke mjere

Sve podatke koji postoje u materijalnom (fizičkom) obliku Muzej čuva u ormarićima, a ključevi se nalaze kod ovlaštenih osoba, što znači da neovlaštene osobe nemaju pristup istima. Takav pristup čuvanju osobnih podataka je u skladu sa zakonom i Uredbom i preporučujemo ubuduće postupati isključivo na takav način, pazeći da pristup imaju samo ovlaštene osobe.

Nadalje, utvrđeno je da se neki osobni podaci prikupljaju i obrađuju na način da se kopira osobna iskaznica i kopija se kao takva pohranjuje na gore opisani način. Iako je utvrđeno da se podaci uglavnom čuvaju sigurno i odgovorno, takvo postupanje u većini slučajeva predstavlja prekomjernu obradu osobnih podataka ispitanika. Naime, osobnom iskaznicom se ispitanik identificira u puno većoj mjeri nego što je to potrebno. Posjedujući kopiju nečije osobne iskaznice otkrivamo identitet te osobe kroz poveći broj osobnih podataka. Stoga, poštujući načela obrade koja su propisana Uredbom, u slučaju kopiranja osobne iskaznice, preporučujemo precrtati odnosno zacrniti sve podatke koji nisu neophodni. Isto vrijedi i za preslike kartica tekućih računa, žiro računa itd.

Obzirom da se velika količina osobnih podataka obrađuje i u fizičkom obliku, preporuka je nabava rezača papira, te u uništavanje dokumenata koji sadrže nečije osobne podatke pomoću rezača umjesto bacanja istih u smeće.

Također, upućujemo na suradnju službenika i dužnosnika sa službenikom za zaštitu osobnih podataka, te preporučujemo podržavanje njegovih aktivnosti i prihvaćanje uputa koje isti daje u sklopu provođenja Uredbe.

Ukoliko se postigne bilo kakav usmeni dogovor u odnosu na obradu osobnih podataka, odnosno ako se prikupi usmena privola, vrlo je važno to dokumentirati kako bi se ista po potrebi mogla dokazati, pa stoga u takvim slučajevima preporučujemo sastaviti službenu bilješku.

Kada se provode natječaji za zapošljavanje, potrebno je razmisliti o narednom korištenju dokumentacije osoba koje nisu izabrane, odnosno kada prestane svrha u koju su osobni podaci dani, u konkretnom slučaju provođenje natječaja, prikupljene osobne podatke je potrebno uništiti, a ukoliko ih želite iz nekog razloga zadržati za daljnju uporabu, za takvo postupanje je potrebno zatražiti privolu.

7. Tablični prikaz preporuka

R.Br.	Poglavlje	Preporuka
	IT-informatički sustav	- Pristup podacima - Održavanje sustava od strane drugih pravnih osoba - Pristup internetu i elektroničkoj pošti - Zaštita podataka - Korištenje računalnih programa - Knjiga standarda informatičke sigurnosti
	Video nadzor	- Izrada pravilnika o provođenju video nadzora usklađenim s Uredbom
	Pravni sustav	- Poštivanje obveza od strane službenika za zaštitu podataka i redovno praćenje propisa - Pohrana izjava o povjerljivosti u osobne dosjee zaposlenika - Sklapanje sporazuma o obradi podataka s izvršiteljima obrade - Unošenje ugovorne odredbe u postojeće ugovore - Korekcija i vođenje evidencije aktivnosti obrade
	Organizacijske i tehničke mjere	- prilagoditi pohranjivanje kopija osobnih iskaznica ispitanika i drugih dokumenata - rezač papira, službene bilješke

8. Zaključak

Uzimajući u obzir provedenu analizu postojećeg stanja, utvrđeno je da Muzej kao voditelj obrade u svom redovnom poslovanju i u okviru svog djelovanja obrađuje određenu količinu osobnih podataka. Između ostalog, utvrđeno je da je Muzej kao voditelj obrade proveo većinu aktivnosti u svrhu usklađenja postupanja sa zahtjevima Uredbe i Zakona o provedbi Opće uredbe o zaštiti podataka, no potrebno je poduzeti još neke radnje kako bi usklađenje bilo kompletno, a koje su detaljnije opisane u pravnim i informatičkim preporukama za daljnje postupanje. Potrebno je donijeti i Pravilnik o korištenju sustava video nadzora.

Razlikujemo 4 faze obrade osobnih podataka: prikupljanje, obradu, pohranu i brisanje. Kod prikupljanja osobnih podataka, prvenstveno je nužno utvrditi koji je pravni osnov takvog postupanja, je li to zakon, privola, nužnost izvršenja ugovora ili drugi Uredbom propisani temelj obrade. Nakon utvrđenja pravnog osnova, također je bitno utvrditi koja je svrha prikupljanja određenih osobnih podataka, pa te podatke upotrebljavati isključivo u tu svrhu, pri čemu je vrlo važno paziti i na opseg prikupljanja osobnih podataka, odnosno prikupiti samo osobne podatke koji su nužni za određenu svrhu. Sve što je prikupljeno izvan toga se smatra prekomjernom obradom osobnih podataka.

Dakle, prije svega potrebno je postupiti sukladno uputama iz ove analize. Pritom je važno imati na umu kako usvajanje pravnih akata i donošenje pravilnika na razini voditelja obrade samo po sebi ne jamči da će se s osobnim podacima postupati sukladno Uredbi. Garancija odgovornog postupanja s osobnim podacima su isključivo redovno praćenje propisa iz područja zaštite osobnih podataka i mišljenja Agencije te preispitivanje i redovan nadzor vlastitog postupanja, odnosno provođenje revizije na godišnjoj razini.

9. Popis priloga

Sastavni dio ove analize su sljedeći prilozi:

1. Upitnik A) Evidencija obrade podataka
2. Upitnik B) Načela i principi