GKR
Gradska knjižnica Rijeka

Rijeka, M. Gupca 23
Tel: 051 211 139
Faks.: 051 338 609
E-mail: gkri@gkri.hr

PROCJENA UČINKA NA ZAŠTITU OSOBNIH PODATAKA

Voditelj obrade: *Gradska knjižnica Rijeka, Matije Gupca 23, OIB: 53791148489*

UVOD

Gradska knjižnica Rijeka je javna ustanova koja u okviru svojih djelatnosti posuđuje knjižničnu građu svojim članovima. Članstvo Gradske knjižnice Rijeka doseže brojku između dvadeset i trideset tisuća aktivnih članova godišnje.

Naslovi i sadržaj knjižnične građe koja se posuđuje mogu ukazivati na politička mišljenja, filozofska i vjerska uvjerenja, podatke koji se odnose na zdravlje ili spolni život, odnosno spolnu orijentaciju članova te kao takvi potencijalno ulaze u posebnu kategoriju osobnih podataka u smislu 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.

S obzirom na navedeni broj aktivnih članova na godišnjoj razini, koja za regiju u kojoj se nalazi Voditelj obrade možebitno predstavlja opsežnu obradu te obradu posebnih kategorija osobnih podataka evidentiranjem posuđene knjižnične građe, provodi se predmetna procjena učinka na zaštitu osobnih podataka u svrhu osiguranja zakonitosti i poštenosti obrade koja predstavlja temeljnu djelatnost Gradske knjižnice Rijeka.

OPĆE ODREDBE

Predmetna procjena učinka na zaštitu osobnih podataka je izrađena u sukladnosti s metodologijom utvrđenom standardom ISO/IEC 29134:2017 te sukladno članku 35. Opće uredbe o zaštiti osobnih podataka i smjernicama radne skupine 29 (Working Party 29).

Cilj predmetne procjene nije utvrditi može li se uopće provoditi obrada osobnih podataka koja je predmet proučavanja, budući da ista predstavlja temeljnu djelatnost javne ustanove čije je poslovanje usmjereno isključivo u društveno poželjne svrhe, već je cilj utvrditi na koji način se tijekom izvršenja djelatnosti može postići najmanji mogući rizik za ispitanike, članove Gradske knjižnice Rijeka.

TEMELJNE DEFINICIJE

„Osobni podaci" su svi podaci koje se odnose na fizičke osobe čiji je identitet utvrđen ili se može utvrditi. Pojedinac čiji se identitet može utvrditi jest pojedinac koji se može identificirati, izravno ili neizravno, prije svega uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili pomoću jedne ili više značajki svojstvenih za fizički, psihološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

„Obrada" je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim ili 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.

„Posebne kategorije osobnih podataka" su podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

„Voditelj obrade" je fizička ili pravna osoba ili drugo tijelo koje, samo ili zajedno s drugima, određuje svrhe i sredstva obrade osobnih podataka.

„Povreda osobnih podataka“ je 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.

„Uredba“ je 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.

„Knjižnica“ je Gradska knjižnica Rijeka, naručitelj predmetne procjene učinka na zaštitu osobnih podataka i voditelj obrade.

REGULATORNI OKVIR PROVOĐENJA PROCJENE UČINKA NA ZAŠTITU OSOBNIH PODATAKA

Člankom 35. Uredbe određeni su slučajevi u kojima je obvezna provođenja procjene učinka na zaštitu osobnih podataka:

1) sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način znatno utječu na pojedinca;

2) opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima;

3) sustavnog praćenja javno dostupnog prostora u velikoj mjeri.

Raspon obrada osobnih podataka za koje se obvezno provodi procjena učinka na zaštitu osobnih podataka je proširena Odlukom o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka, koju je izdala Agencija za zaštitu osobnih podataka, hrvatsko nadzorno tijelo, dana 21. prosinca 2018. godine. Sukladno navedenoj Odluci, provedba procjene učinka na zaštitu osobnih podataka je obvezna kod obrade u sljedećim slučajevima:

1) Obrada osobnih podataka radi sustavnog i opsežnog profiliranja ili automatiziranog odlučivanja kako bi se donijeli zaključci koji u značajnoj mjeri utječu ili mogu utjecati na pojedinca i/ili više osoba ili koji služe kao pomoć u donošenju odluka o nečijem pristupu nekoj usluzi ili servisu ili pogodnosti (npr. kao što je obrada osobnih podataka odnosnih na ekonomski ili financijski status, zdravlje, osobne preferencije, interese, pouzdanost, ponašanje, podatke o lokaciji i dr.);

2) Obrada posebnih kategorija osobnih podataka u svrhu profiliranja ili automatiziranog odlučivanja;

3) Obrada osobnih podataka djece u svrhu profiliranja ili automatiziranog odlučivanja ili za marketinške svrhe, ili za izravnu ponudu usluga namijenjenu njima;

4) Obrada osobnih podatka prikupljenih od trećih strana koji se uzimaju u obzir za donošenje odluke vezane za sklapanje, raskidanje, odbijanje ili produženje ugovora o pružanju usluga fizičkim osobama;

5) Obrada posebnih kategorija osobnih podataka ili osobnih podataka o kaznenoj ili prekršajnoj odgovornosti u velikom opsegu;

6) Obrada osobnih podataka korištenjem sustavnog nadzora javno dostupnih mjesta u velikom opsegu;

7) Uporaba novih tehnologija ili tehnoloških rješenja za obradu osobnih podatka ili sa mogućnošću obrade osobnih podataka (npr. primjena „interneta stvari", poput pametnih televizora, pametnih kućanskih aparata, komunikacijski povezanih igračaka, sustava „pametni gradovi", pametnih mjerača energije, itd.) koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih osoba;

8) Obrada biometrijskih podataka kad je ispunjen bar još jedan kriterij iz Smjernica o procjeni učinka na zaštitu podataka (WP 248 rev. 01) koji služe za procjenu hoće li određeni postupci obrade vjerojatno prouzročiti visok rizik za prava i slobode ispitanika;

9) Obrada genetskih podataka kad je ispunjen bar još jedan kriterij iz Smjernica o procjeni učinka na zaštitu podataka (WP 248 rev. 01) koji služe za procjenu hoće li određeni postupci obrade vjerojatno prouzročiti visok rizik za prava i slobode ispitanika;

10) Obrada osobnih podataka povezivanjem, usporedbom ili provjerom podudarnosti iz više izvora;

11) Obrada osobnih podataka na način koji uključuje praćenje lokacije ili ponašanja pojedinca u slučaju sustavne obrade komunikacijskih podataka (metapodaci) nastalih uporabom telefona, interneta ili drugih komunikacijskih kanala, kao što je GSM, GPS, Wi Fi, praćenje ili obrada podataka o lokaciji;

12) Obrada osobnih podataka korištenjem uređaja i tehnologija kod kojih incidentni događaj može ugroziti zdravlje pojedinca ili više osoba;

13) Obrada osobnih podataka zaposlenika uporabom aplikacija ili sustava za praćenje (npr. kao što je obrada osobnih podatka za praćenje rada, kretanja, komunikacije i sl.).

S obzirom na to da obrada koju vrši Knjižnica možebitno spada u istu odredbu, određenu točkom 2. navedenog čl. 35 Uredbe, odnosno u točku 5. Odluke Agencije za zaštitu osobnih podataka, ravnatelj Knjižnice je odlučio u suradnji sa službenikom za zaštitu osobnih podataka pristupiti provedbi procjene učinka na zaštitu osobnih podataka.

OBRADA OSOBNIH PODATAKA ČLANOVA KNJIŽNICE

Svrhe obrade i popis osobnih podataka

Osobni podaci članova Knjižnice se obrađuju radi osiguranja povrata posuđene knjižnične građe te naplate potraživanja nastalih uslijed gubitka ili nepravovremenog povrata posuđene građe. Dodatno, uz temeljnu djelatnost Knjižnice, pružaju se i sporedne usluge tijekom kojih se obrađuju osobni podaci.

Sporedne usluge su primjerice obavještavanje članova o pristizanju nove knjižnične građe, organiziranje prezentiranja knjiga i drugih srodnih događaja, fotografiranje istih događaja te pohrana povijesti posudbe pojedinih korisnika.

Popis osobnih podataka koji se obrađuju:

- Ime i prezime
- Adresa prebivališta i boravišta
- Osobni identifikacijski broj
- Datum upisa
- Godina rođenja

Ukoliko pojedini član izrazi privolu mogu biti obrađivani i sljedeći podaci:

- Telefonski broj
- E-mail adresa
- Povijest posudbe

Pravna osnova obrade

Osobni podaci korisnika koji su nužni za upisivanje članstva u Knjižnici se obrađuju temeljem zakonske obveze Knjižnice da zaštiti vlastitu knjižničnu građu sukladno Zakonu o knjižnicama i knjižničnoj djelatnosti, a takva zaštita vlastite imovine zasigurno predstavlja i legitimni interes Knjižnice. Nadalje, takva obrada je i nužna za izvršavanje zadaće od javnog interesa, a što obavljanje knjižnične djelatnosti zasigurno jest.

Temeljem jasne, slobodno dane i izričite privole se mogu obrađivati telefonski broj, e-mail adresa i povijest posudbi člana. Povijest posudbe se obrađuje kako bi član mogao dobiti informaciju o tome koje je knjige već posuđivao, odnosno čitao, a koje nije. Čak i temeljem privole takvi podaci se ne čuvaju na razdoblje dulje od pet godina te je član, ukoliko želi zadržati mogućnost pregleda povijesti posudbe, dužan svake godine prilikom učlanjenja izraziti privolu za takvu obradu.

Relevantnost obrade za poslovanje Knjižnice

Obrada osobnih podataka članova radi evidentiranja kod kojih se članova nalaze dijelovi građe predstavlja *conditio sine qua non* održivosti poslovanja Knjižnice te se izostankom takvog evidentiranja ne bi moglo na duže staze obavljati djelatnost javne knjižnice, budući da bi se fond knjižnične građe rasuo u kratkom vremenu uslijed izostanka povrata građe od strane članova.

Također, bitan dio poslovanja Knjižnice su i zakasnine koje stimuliraju članove na kraće zadržavanje građe te predstavljaju i prihod za Knjižnicu uslijed nepravovremenog povrata.

Uzevši u obzir sve navedeno, u svrhu održavanja javnih knjižnica **nužno je** da se evidentiraju njezini članovi s dostatnom količinom osobnih podataka za naplatu u slučaju nastanka štete, gubitka knjižnične građe ili njezinog nepravovremenog povrata.

Način i metode obrade osobnih podataka

Obrada osobnih podataka članova započinje prikupljanjem izravno od ispitanika zaprimanjem popunjene upisnice u pojedinim odjelima. Podaci se s papirnate upisnice unose u informatički sustav Knjižnice, točnije u radnom programu naziva „ZAKI". Papirnate upisnice se zatim pohranjuju u ormarima kojima je pristup osiguran zaključavanjem ugrađenih brava.

Budući da se u daljnjim fazama obrada odvija gotovo isključivo unutar radnog programa „ZAKI", obrazložiti će se o kakvom se programu radi. Program je nastao kao proizvod suradnje Kataloga Knjižnica grada Zagreba i trgovačkog društva VIVA INFO d.o.o., sa sjedištem u Zagrebu, Nova cesta 46, OIB: 22361751585.

U programu je moguće vidjeti sve osobne podatke članova sadržane u upisnici. Sukladno utvrđenoj politici Knjižnice, razdoblje pohrane tih osobnih podataka jest godinu dana od dana isteka članstva, odnosno do zastarnih rokova ili okončanja sudskih ili istovrijednih postupaka u slučaju neispunjenja obveza člana prema Knjižnici.

Pristup radnom programu je zaštićen korisničkim imenom i lozinkom. Izrađuju se sigurnosne kopije pohranjenih podataka radi očuvanja cjelovitosti i povjerljivosti. Informatički sustav Knjižnice se periodično podvrgava testiranju, a računala su opremljena antivirusnim programom i firewallom.

Radi uređenja odnosa o povjerljivosti osobnih podataka članova, a i sukladno zahtjevima Uredbe, s izvršiteljem obrade VIVA INFO d.o.o. je sklopljen ugovor o obradi osobnih podataka. Uspostavljen je automatizirani sustav zapisa za evidentiranje pristupa sustavu

koji će sadržavati vrijeme i mjesto pristupa te oznaku osobe koja je izvršila izmjenu osobnih podataka.

Radnici koji obrađuju osobne podatke članova su prošli edukaciju o važećim propisima o zaštiti osobnih podataka te se izjavama o povjerljivosti obvezali Knjižnici kako iste neće obrađivati na nezakonite načine.

Također, radi detaljnijeg upućivanja radnika po pitanju zaštite osobnih podataka Knjižnica je usvojila politike zaštite osobnih podataka, koji predstavlja provedbeni akt kojeg radnici mogu konzultirati u svako doba za slučaj nedoumica u obradi osobnih podataka.

Nadalje, radi pružanja adekvatnog stupnja stručne potpore po pitanjima zaštite osobnih podataka, Knjižnica je angažirala vanjskog službenika za zaštitu osobnih podataka, Odvjetničko društvo Kovačević, Koren i partneri d.o.o. iz Rijeke, Frana Supila 6/III radi savjetovanja u tom pravnom području i izrade potrebnih dokumenata za Knjižnicu.

Rizik vezan uz obradu

Rizik će se procijeniti vršeći kvalitativnu analizu rizika u skladu sa standardom ISO/IEC 29134:2017.

Uvodno, radi ispravne procjene rizika korisno je izvršiti i povijesni pregled obrade osobnih podataka od strane Knjižnice. Najveća opasnost za članove leži u eventualnoj javnoj objavi posebnih kategorija osobnih podataka članova. Takvih povreda osobnih podataka članova u dosadašnjem poslovanju nije bilo, iako je s računalnim poslovanjem u radu s korisnicima Knjižnica započela još 1993. godine, a niti se bilježi kakva druga slična povreda vezana uz papirnatu pohranu dokumenata. Ovakva povijest bez grubih povreda predstavlja bitan faktor pri procjeni rizika za buduće povrede.

Također, nužno je istaknuti i kako Knjižnica evidentira samo naslove knjiga koje su članovi posudili, a što u stvarnosti ne dovodi do zaključka da je ista uopće pročitana, a kamoli da su usvojena politička mišljenja, odnosno vjerska ili filozofska uvjerenja u njima sadržana.

Naslovi knjiga vezanih za zdravlje potencijalno upućuju na zdravlje samog člana, međutim izvjesno je kako se i brojne takve knjige posuđuju radi zdravstvenih problema bližnjih, radi čega se ne može izvući neposredan zaključak o zdravstvenom stanju osobe, već se samo može uspostaviti veza s određenim stupnjem vjerojatnosti.

Sukladno navedenom ISO standardu, utvrđene su vrijednosti na temelju kojih se utvrđuje vjerojatnost rizika i razina utjecaja na ispitanika kako slijedi:

LJESTVICA VJEROJATNOSTI RIZIKA		
1	Niska	Vjerojatnost ostvarivanja prijetnje čini se zanemariva
2	Srednja	Vjerojatnost ostvarivanja prijetnje čini se ograničena
3	Visoka	Vjerojatnost ostvarivanja prijetnje čini se značajna
4	Vrlo visoka	Vjerojatnost ostvarivanja prijetnje čini se maksimalna

LJESTVICA RAZINE UTJECAJA NA ISPITANIKA		
1	Niska	Razina utjecaja čini se zanemariva (iritacija, ponovni unos podataka, smetnje)
2	Srednja	Razina utjecaja čini se ograničena (dodatni troškovi, strah, stres, manje fizičke nelagode)
3	Visoka	Razina utjecaja čini se značajna (imovinska šteta, gubitak sredstava s računa, pogoršanje zdravlja)
4	Vrlo visoka	Razina utjecaja čini se maksimalna (smrt, dugotrajne fizičke i psihičke poteškoće, prouzročenje nesposobnosti za rad)

UTVRĐIVANJE RIZIKA				
	Niska vjerojatnost	Srednja vjerojatnost	Visoka vjerojatnost	Vrlo visoka vjerojatnost
Niska razina utjecaja	1	2	3	4
Srednja razina utjecaja	2	4	6	8
Visoka razina utjecaja	3	6	9	12
Vrlo visoka razina utjecaja	4	8	12	16

Razine rizika:

- Zanemariv rizik (1-2)
- Marginalan rizik (3-4)
- Značajan rizik (6-9)
- Kritičan rizik (12-16)

Rizik	Implementirane zaštitne mjere	Prijetnja
Neovlašteni pristup osobnim podacima	Pristup radnom programu je osiguran korisničkim imenom i lozinkom, papirnati podaci se pohranjuju u zaključanim ormarima	Izostanak zatvaranja radnog programa pri udaljavanju od računala
Neovlaštena izmjena osobnih podataka	Automatizirani sustav zapisa uz primjenu mjera informatičke sigurnosti protiv neželjenih izmjena	
Neovlaštena zloupotreba, gubitak ili krađa	Potpisani ugovori sa svim izvršiteljima obrade te prikupljene izjave o povjerljivosti od radnika	Nedostatak modernih informatičkih zaštitnih mjera (pseudonimizacija, enkripcija)
Prekomjerno prikupljanje osobnih podataka	U suradnji sa službenikom za zaštitu osobnih podataka proučeni i prilagođeni svi radni procesi radi minimiziranja prikupljenih osobnih podataka	Brisanje podataka članova ne ovisi isključivo o Knjižnici, već se isto mora zatražiti od strane VIVA INFO d.o.o., radi čega su moguće odgode u postupku brisanja
Nedostatna obaviještenost	Svi ispitanici su uredno obaviješteni o obradi prilikom popunjavanja upisnice i putem pravila privatnosti na web stranici Knjižnice	
Nepridržavanje pravila voditelja obrade	Izjave o povjerljivosti radnika osobno obvezuju na pridržavanje pravilima	

Rizik	Vjerojatnost	Posljedica	Razina rizika
Neovlašteni pristup osobnim podacima	1	2	2
Neovlaštena izmjena osobnih podataka	1	2	2
Neovlaštena zloupotreba, gubitak ili krađa	2	2	4
Prekomjerno prikupljanje osobnih podataka	1	2	2
Nedostatna obaviještenost	1	1	1
Nepridržavanje pravila voditelja obrade	1	2	2

Zaključak

Analizom rizika utvrđeno je kako su svi rizici vezani uz obradu osobnih podataka članova Knjižnice zanemarivi ili marginalni. S obzirom da je najviša vrijednost rizika zabilježena kod neovlaštene zloupotrebe, gubitka ili krađe, sukladno ograničenjima vlastitih sredstava, nastojati će se u tijeku daljnjeg poslovanja Knjižnice, a ovisno o financijskim mogućnostima iste, umanjiti navedeni rizik na način da se u postojeći radni program implementira mogućnost enkripcije ili pseudonimizacije članova, odnosno da se pristupi izradi novog radnog programa koji bi omogućio takvu zaštitnu mjeru. S obzirom na sve navedeno, predlaže se da se navedeni rizici prihvate.

Iz predmetne procjene je razvidno da Knjižnica, sukladno svojim organizacijskim i financijskim mogućnostima poduzima sve moguće korake za pružanje zaštite osobnih podataka vlastitim članovima. Također, nužno je istaknuti kako je predmetna obrada nužna za ostvarivanje ciljeva Knjižnice, a koji ciljevi ujedno predstavljaju i javni interes lokalne zajednice. Iz svega navedenog proizlazi kako obrada ne predstavlja rizik za prava i slobode pojedinaca.

Ravnatelj

Niko Cvjetković

Broj: 282/2018

Rijeka, 25. svibnja 2018. godine