

Delovodni broj: 194/23
Datum: 28.03.2023. godine

POLITIKA ZAŠTITE PODATAKA O LIČNOSTI

Beograd, 2023.

Sadržaj

- 1. Namena, obim i korisnici**
- 2. Referentna dokumenta**
- 3. Definicije termina**
- 4. Osnovna načela obrade podataka o ličnosti**
 - 4.1. Zakonitost, poštenje i transparentnost
 - 4.2. Ograničenje namene
 - 4.3. Minimizacija podataka
 - 4.4. Tačnost
 - 4.5. Ograničen period čuvanja
 - 4.6. Integritet, poverljivost i raspoloživost
 - 4.7. Kontrolisana odgovornost (Accountability)
- 5. Izgradnja sistema zaštite podataka u Školi**
 - 5.1. Obaveštavanje fizičkog lica
 - 5.2. Izbor i pristanak fizičkog lica
 - 5.3. Skupljanje podataka
 - 5.4. Upotreba, zadržavanje i odlaganje podataka
 - 5.5. Otkrivanje podataka trećim stranama
 - 5.6. Prekogranični prenos podataka o ličnosti
 - 5.7. Prava pristupa fizičkog lica podacima
 - 5.8. Prenosivost podataka o ličnosti
 - 5.9. Pravo na zaborav (brisanje podataka)
 - 5.10. Odgovornost i nadoknada štete
- 6. Smernice za poštenu obradu podataka o ličnosti**
 - 6.1. Obaveštenje o privatnosti za fizička lica
 - 6.2. Dobijanje pristanka
- 7. Organizacija i odgovornosti**
- 8. Smernice za uspostavljanje vodećeg nadzornog tela**
 - 8.1. Neophodnost uspostavljanja vodećeg nadzornog tela
 - 8.2. Glavno sedište Škole i vodeće nadzorno telo
 - 8.2.1. Glavno sedište rukovaoca podataka o ličnosti
 - 8.2.2. Glavno sedište obrađivača podataka o ličnosti
- Odgovor na incident povrede podataka o ličnosti**
- 9. Provera i odgovornost**
- 10. Menadžment održavanja zapisa politike**
- 11. Validacija i menadžment dokumenta**
 - 13.1. Validaciju ove politike vrše vlasnik (staratelj) ove politike, Lice za zaštitu podataka o ličnosti (DPO) i Direktor koji mora kontrolisati i proveravati primenu politike o zaštiti privatnosti, a Lice za zaštitu podataka o ličnosti po potrebi i ažurirati dokument najmanje jedanput godišnje.
 - 13.2. Ova politika stupa na snagu danom potpisivanja: 29.12.2022. godine.

1. Namena, obim i korisnici

Srednja škola za informacione tehnologije, ul. Cara Dušana br. 34, opština Zemun, Beograd, PIB: 107149043, matični broj: 17805037 (u nastavku "**Škola**"), namerava da se usaglasi sa primenljivim zakonima i regulativama Republike Srbije koje se odnose na zaštitu podataka o ličnosti. Ova politika ističe osnovne principe obrade ličnih podataka učenika, zakonskih zastupnika, zaposlenih i drugih pojedinaca ili predstavnika zakona (u nastavku „**Korisnici**“) i ukazuje na odgovornosti Škole i zaposlenih u aktivnostima obrade podataka. Ova politika se primenjuje na Školu i njena izdvojena odeljenja.

2. Referentna dokumenta

- *Zakon o zaštiti podataka o ličnosti*
- *Zakon o informacionoj bezbednosti Republike Srbije*, „Sl. Glasnik RS“, br. 6/2016
- *Zakon o obligacionim odnosima Republike Srbije*, ("Sl. list SFRJ", br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, "Sl. list SRJ", br. 31/93 i "Sl. list SCG", br. 1/2003 - Ustavna povelja)

3. Definicije termina

Definicije termina korišćene u ovom dokument su sadržane u Članu 4 *Zakona o zaštiti podataka o ličnosti* (u daljem tekstu; **Zakona**):

Podaci o ličnosti: Svaka informacija koja se odnosi na identifikaciju ili lične identifikacione informacije fizičkih lica (*lica na koje se podaci odnose*) koja mogu biti direktno ili indirektno identifikovana, posebno na osnovu nekog identifikatora kao što je ime, lični broj, podatak o lokaciji, ili jedan ili više faktora specifičnih za fizički, psihološki, genetski, mentalni, ekonomski, kulturološki ili društveni identitet fizičkog lica.

Osetljivi podaci o ličnosti: Podaci o ličnosti koji po svojoj prirodi, posebno osetljivosti za prava i slobode lica na koja se podaci odnose, zaslužuju specifične mere zaštite pošto kontekst (aktivnosti) obrade podataka može izazvati visok rizik za fundamentalna prava i slobode fizičkih lica. Ovi podaci uključuju rasnu ili etičku pripadnost, religijsko ili filozofska uverenje, genetičke podatke, biometrijske podatke za jedinstvenu identifikaciju fizičkih lica.

Rukovalac podataka: Fizičko ili pravno lice, predstavnik javne vlasti, agencija ili drugo telo koje samo ili zajedno određuje namenu i sredstva obrade ličnih podataka.

Obradivač podataka: Fizičko ili pravno lice, predstavnik javne vlasti, agencija ili drugo telo koje obrađuje lične podatke u ime kontrolora.

Obrada: Svaka operacija ili skup operacija koje se izvršavaju nad ličnim podacima ili skupu ličnih podataka, manuelnim ili automatizovanim sredstvima, kao što su: *skupljanje, snimanje, organizacija, struktuiranje, pohranjivanje, adaptacija ili izmena, izvlačenje, konsultovanje, upotreba, otkrivanje prenosom, distribucija ili stavljanje na raspolaganje na drugi način, usklađivanje ili kombinovanje, restrikcija, brisanje ili uništavanje podataka*.

Anonimizacija (sinonim: **šifrovanje**) : Nepovratan proces naknadne identifikacije ličnih podataka tako da fizičko lice ne može biti identifikovano u razumnom vremenu, sa razumnim troškovima i tehnologijom bilo od strane rukovaoca ili drugih lica za identifikaciju tog lica. Principi obrade ličnih podataka ne primenjuju se na anonimizovane podatke koji nisu više podaci o ličnosti lični.

Pseudonimizacija (sinonim: **kodiranje**): Obrada ličnih podataka na takav način da na dalje ne može biti povezan sa specifičnim fizičkim licem bez upotrebe dodatnih informacija. Takve dodatne informacije moraju da se drže odvojeno i da su zaštićene tehničkim i organizacionim merama koje osiguravaju da se podaci o ličnosti ne mogu pridružiti fizičkom licu. Pseudonimizacija smanjuje, ali ne eliminiše potpuno sposobnost povezivanja ličnih podataka sa fizičkim licem na koga se podaci odnose. Ovi podaci su još uvek lični podaci i na njih se odnose načela obrade ličnih podataka.

Nadzorno telo (*Supervisory Authority*): Nezavisno javno telo koje je uspostavljeno u državama članicama EU prema članu 51 EU GDPR i u Republici Srbiji prema Članu 73 Zakona - Poverenik.

4. Osnovna načela obrade podataka o ličnosti

Načela (principi) zaštite podataka opisuju osnovne odgovornosti organizacije koja rukuje podacima o ličnosti. Prema članu 4 tačka 8) Zakona rukovalac (kontrolor) „je fizičko ili pravno lice, odnosno organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade. Zakonom kojim se određuje svrha i način obrade, može se odrediti i rukovalac ili propisati uslovi za njegovo određivanje“.

4.1. Zakonitost, poštenje i transparentnost

Podaci o ličnosti moraju se skupljati i obrađivati zakonito, pošteno i transparentno u odnosu na lice na koje se podaci odnose (GDPR princip "zakonitosti, poštenja i transparentnosti"). Zakonita obrada je obrada koja se vrši u skladu sa ovim Zakonom, Član 5(1), odnosno drugim zakonom kojim se uređuje obrada.

4.2. Ograničenje namene

Podaci o ličnosti moraju se prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama (na primer, profilisanje i marketing) ("ograničenje u odnosu na svrhu obrade", Zakon, član 5(2)).

4.3. Minimizacija podataka

Lični podaci skupljani, obrađivani i pohranjivani u Školi moraju biti adekvatni, relevantni i ograničeni na minimalnu količinu koja je neophodna za namene za koje su skupljani, obrađivani i pohranjivani. Škola mora primeniti anonimizaciju ili pseudonimizaciju podataka o ličnosti ako postoji visok rizik za prava i slobode fizičkih lica i mogućnost da se smanji rizik za fizička lica.

4.4. Tačnost

Podaci o ličnosti skupljeni u Školi moraju biti tačni i, gde je neophodno, ažurno održavani. Škola će preduzeti racionalne korake da se netačni lični podaci, imajući u vidu namenu za koju su skupljeni i obrađivani, blagovremeno izbrišu ili isprave (Zakon, član 5(4)).

4.5. Ograničen period čuvanja

Lični podaci će se čuvati u Školi u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade ("ograničenje čuvanja", Zakon, član 5(5)).

4.6. Integritet, poverljivost i raspoloživost

Uzimajući u obzir poslednju tehnologiju i druge raspoložive mere zaštite podataka i informacija, troškove implementacije i verovatnoću i intenzitet rizika za lične podatke, Škola mora primeniti odgovarajuće tehničke i organizacione mere za obradu ličnih podataka na način koji osigurava odgovarajuću bezbednost ličnih podataka, uključujući raspoloživost kada su potrebni i zaštitu od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog pristupa ili otkrivanja (Zakon, član 5(6)).

4.7. Kontrolisana odgovornost

Direktor Škole kao rukovalac (kontrolor) podataka je odgovoran i sposoban da demonstrira usaglašenost sa gore opisanim načelima Zakona zaštite podataka o ličnosti.

5. Izgradnja sistema zaštite podataka u Školi

Da bi demonstrirala usaglašenost sa načelima zaštite podataka o ličnosti Zakona, Škola će ugraditi sistem zaštite podataka u poslovne procese i aktivnosti.

5.1. Obaveštavanje fizičkog lica

Škola mora objaviti *Obaveštenje o privatnosti* na web sajtu i napraviti link prema ovoj Politici. *Obaveštenje o privatnosti* treba da sadrži sve neophodne informacije koje se odnose na skupljanje podataka, aktivnosti obrade, vreme zadržavanja podataka, mere zaštite podataka, lokaciju obrade, odgovornosti itd. (videti sekciju 6.1 Politike).

5.2. Izbor i pristanak fizičkog lica

U poslovanju Škole fizička i pravna lica (lica na koja se podaci odnose) daju eksplicitno svoj pristanak za skupljanje i obradu njihovih ličnih podataka u zakonski uzajamno prihvaćenim i potpisanim komercijalnim ili nekomercijalnim ugovorima (videti 6.2 sekciju Politike) i ostalih komercijalnih ugovora.

5.3. Skupljanje podataka

Škola mora nastojati da skuplja što je manju moguću količinu ličnih podataka. Ako lične podatke u ime Škole skuplja treća strana Lice za zaštitu podataka o ličnosti, ili lice zaduženo za zaštitu podataka o ličnosti u Školi, mora osigurati da se lični podaci skupljaju na zakonskoj osnovi.

5.4. Upotreba, zadržavanje i odlaganje podataka

Namene i metodi obrade, ograničeno pohranjivanje i zadržavanje ličnih podataka mora biti konzistentno sa informacijama sadržanim u *Obaveštenju o privatnosti*. Škola će održavavati tačnost, integritet, poverljivost, raspoloživost i relevantnost podataka o ličnosti kroz sve aktivnosti namenjene obrade. Adekvatni mehanizmi tehničke i organizacione zaštite projektovani su u Školi da štite lične podatke od krađe, pogrešne upotrebe ili zloupotrebe i spreče proboj ličnih podataka. Direktor Škole je odgovoran za usaglašenost navedenu u ovoj sekciji:

1. Kopiranje ili dupliranje podataka nikada se ne sme vršiti bez znanja Direktora, sa izuzetkom stvaranja rezervnih kopija, osim dok je neophodno za osiguranje namenjene obrade, kao i za regulatorno zadržavanje podataka.
2. Posle zaključivanja rada po ugovoru ili SLA (Service-level agreement), ili ranije po zahtevu Škole, a najkasnije po završetku ugovornih ili SLA obaveza, Škola će na zahtev prethodnog pristanka klijenta, izbrisati, ili šifrovati (anonimizovati) podatke i arhivirati zajedno sa ugovorima i SLA za čuvanje u zakonskom periodu (do 10 godina) ili po potrebi duže.
3. Dokumentacija koja je korišćena da demonstrira regularnu obradu podataka u skladu sa ugovormo i SLA, Škola će pohraniti i čuvati duže od perioda trajanja ugovora i SLA u skladu sa odgovarajućim zakonskim periodom zadržavanja.

5.5. Otkrivanje podataka trećim stranama

Kad god Škola koristi poverljivu treću stranu (dobavljača ili poslovnog partnera) da obrađuje podatke o ličnosti u njeno ime, Lice za zaštitu podataka o ličnosti ili imenovano lice za poslove zaštite ličnih podataka, mora osigurati da će obrađivač obezbediti adekvatne tehničke i organizacione mere zaštite podataka o ličnosti koje su proporcionalne procenjenom riziku. Za ovu svrhu mogu se koristiti *Politika zaštite privatnosti treće strane* (dobavljača) i *usaglašen upitnik o zahtevima zaštite za treću stranu*.

Škola mora ugovorom zahtevati od treće strane (dobavljača ili poslovnog partnera) da obezbedi isti nivo zaštite privatnosti i bezbednosnih mera za zaštitu ličnih podataka. Dobavljač ili poslovni partner moraju obrađivati lične podatke samo da ispune svoje ugovorne obaveze prema Školi ili na osnovu instrukcije koja može sadržavati zakonske, legitimne i druge interese Škole i nikako za druge svrhe. Ako dobavljač obrađuje lične podatke zajedno sa nezavisnom trećom stranom od poverenja, Škola mora eksplicitno specificovati njihove odgovornosti, a treća strana dobavljača mora potpisati relevantan ugovor ili SLA ili drugi legalni obavezujući dokument, kao što je *Sporazum o obradi podataka sa dobavljačem*:

1. Dobavljač će osigurati da Škola može verifikovati usaglašenost sa obavezama dobavljača u skladu sa članom 26 Zakona. Dobavljač (na primer iz zemlje EU) će na zahtev Škole dostaviti neophodne informacije o tehničkoj i organizacionoj zaštiti podataka i, posebno, demonstrirati primenu tehničkih i organizacionih mera zaštite podataka. Dokaz o primeni ovih mera može se obezbediti usaglašavanjem sa kodeksom postupanja u skladu sa čl. 59 Zakona;
2. Sertifikatom usaglašenosti sa odobrenom procedurom sertifikacije prema Članu 61, Zakona;
3. Važećim sertifikatom o proveri, izveštajem ili delom izveštaja obezbeđenog od strane nezavisnog tela (na primer: Lica za zaštitu podataka o ličnosti, Odeljenja IT sektora za informacionu bezbednost, inspektora (proverivača) za proveru zaštite privatnosti podataka, ili proverivača sistema kvaliteta);
4. Odgovarajućim sertifikatom od strane internog ili nezavisnog tima za sertifikaciju informacione bezbednosti (na primer ISO/IEC 27001);
5. Gde je, u pojedinačnim slučajevima, neophodna provera i kontrola Škole ili proverivača kojeg Škola postavi, takva provera i kontrola mora se vršiti u radno vreme i bez interferencije sa operacijama dobavljača, na osnovu prethodnog obaveštenja i posmatranjem odgovarajućeg perioda na koji se obaveštenje odnosi. Dobavljač može takođe odrediti da je takva provera i kontrola predmet prethodnog obaveštenja, opservacije odgovarajućeg perioda za koji se obaveštenje daje i izvršavanje preduzetih mera poverljivosti za zaštitu podataka drugih kupaca ili dobavljača i poverljivosti implementiranih tehničkih i organizacionih mera i mera samozaštite. Dobavljač je ovlašćen da odbije proverivače koji su konkurencija dobavljaču;
6. Gde za Školu inspekciju vrši nadzorni organ za zaštitu podataka o ličnosti ili drugi ovlašćeni organ sa statutarnim kompetencijama, gornji paragraf 3 će se primeniti sa mogućnošću neophodnih izmena. Izvršavanje preduzetih mera zaštite poverljivosti neće se zahtevati, ako takvo nadzorno telo ima profesionalnu ili statutarnu obavezu zaštite poverljivosti čije je kršenje predmet sankcija prema primenljivom krivičnom zakonu.

5.6. Prekogranični prenos podataka o ličnosti

Pre prenosa ličnih podataka izvan evropske ekonomske zone (EEA) kao i iz Republike Srbije (Član 63, Zakona) moraju se koristiti adekvatne mere samozaštite obezbeđene u standardnom članu Ugovora, uključujući potpisivanje *Ugovor o prenosu podataka*, kako EU GDPR i Zakon zahtevaju, i u situacijama gde to drugi propisi zahtevaju, sa dobijenim ovlašćenjem lokalnog nadležnog tela za zaštitu podataka (*Poverenik za zaštitu podataka o ličnosti u Srbiji*). Entitet koji prima lične podatke mora se usaglasiti sa skupom principa obrade ličnih podataka opisanih u proceduri *Prekograničnog prenosa podataka koju propisuje Poverenik*.

Opšta načela prenosa podataka (Član 63, Zakona):

Svaki prenos ličnih podataka koji podležu obradi ili su namenjen za obradu posle prenosa u treću zemlju ili u neku međunarodnu organizaciju izvršiće se samo ako, podležu drugim odredbama (čl. 64, 65. i 67. ovog Zakona), ako su uslovi postavljeni u ovom poglavlju usaglašeni sa rukovaocem i obrađivačem, uključujući i za dalji prenos ličnih podataka iz jedne treće zemlje

ili međunarodne organizacije u drugu treću zemlju ili međunarodnu organizaciju. Sve odredbe u ovom poglavlju biće primenjene da bi se osigurao nivo zaštite fizičkih lica zagaranovan Zakonom. Rukovalac je odgovoran da vodi evidenciju o prenosu podataka o ličnosti u druge države ili međunarodne organizacije (Član 47 tačka 5) Zakona), uključujući i naziv druge države ili međunarodne organizacije, kao i dokumente o primeni mera zaštite ako se podaci prenose u skladu sa članom 69. stav 2. ovog Zakona.

Prenos podataka podleže odgovarajućim merama samozaštite (Član 64 Zakona):

1. U odsustvu odluke prema članu 64 tačka 3) Zakona, neki rukovalac ili obrađivač može preneti lične podatke u neku treću zemlju ili neku međunarodnu organizaciju, samo ako je kontrolor ili obrađivač obezbedio odgovarajuće mere samozaštite (Član 65 Zakona), i pod uslovom da su raspoložive mere koje nameću prava lica na koja se podaci odnose i efektivni pravni lek za otklanjanje posledica.
2. Odgovarajuće mere samozaštite navedene u paragrafu 1 mogu se obezbediti, bez zahteva bilo kojeg specifičnog ovlašćenja, od nadzornog organa, sa:
 - (a) Zakonskim obavezujućim i instrumentom koji nameće obavezu izvršavanja sa javnom vlasti ili nadležnim telom;
 - (b) Obavezujućim organizacionim pravilima za evidenciju radnji obrade u skladu sa članom 47 Zakona;
 - (c) Standardnim klauzulama zaštite podataka usvojenim od strane EU Komisije u skladu sa procedurom ispitivanja navedenom u Članu 93(2) GDPR i Članu 50, Zakona;
 - (d) Standardnim klauzulama zaštite podataka usvojenim od nadzornog organa i odobrenog od EU Komisije prema Članu 93(2) GDPR i Članu 51 Zakona;
 - (e) Odobrenim kodom kontrola zaštite prema Članu 59, Zakona zajedno sa obavezujućim i nametnutim angažovanjem rukovaoca i obrađivača u trećoj zemlji za primenu adekvatnih mera samozaštite, uključujući zaštitu prava vlasnika ličnih podataka; ili
 - (f) Odobren mehanizam sertifikacije prema Članu 61 Zakona zajedno sa obavezujućim i nametnutim angažovanjem rukovaoca i obrađivača u trećoj zemlji za primenu odgovarajućih mera samozaštite, uključujući zaštitu prava fizičkih lica.

5.7. Prava pristupa fizičkog lica podacima

Kada radi kao rukovalac (kontrolor) podataka, Direktor Škole je odgovoran da obezbedi licu na koje se podaci odnose pogodan mehanizam za pristup koji mu omogućava da pristupi svojim ličnim podacima i dozvoli mu da ažurira, ispravi, izbriše ili prenese svoje podatke o ličnosti, ako odgovara ili se zahteva po zakonu. Mehanizam za pristup fizičkih lica na koje se podaci o ličnosti odnose biće detaljnije opisan u *Proceduri za zahtev fizičkih lica za pristup podacima* (koju propisuje Poverenik) i obezbeđen uz manuelnu pomoć administratora IKT sistema Škole.

5.8. Prenosivost podataka o ličnosti

Na pisani zahtev lica na koje se podaci odnose, Škola će besplatno dostaviti kopiju podataka koje je dobila od lica, u struktuiranom formatu, ili je preneti drugom rukovaocu. Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti će takav zahtev obraditi u roku od mesec dana od dana podnošenja pisanog zahteva, ako zahtev nije prekomeran (svakodnevan) i ako ne utiče na prava i podatke o ličnosti drugih lica.

5.9. Pravo na zaborav (brisanje podataka)

Fizičko lice na koje se podaci odnose može zahtevati brisanje svojih ličnih podataka (Čl. 30, Zakona). Kada Škola radi kao rukovalac, Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti preduzeće neophodne akcije (uključujući i tehničke mere) da

o zahtevu informiše sve treće strane koje koriste ili obrađuju podatke i u razumnom roku (8 do 16 dana) izbriše zahtevane podatke.

5.10. Odgovornost i nadoknada štete

U slučaju prigovora ili nanete štete za prava i slobode fizičkih lica, Škola i klijent (dobavljač, partner) će biti odgovorni licu na koje se podaci odnose, u skladu sa Zakonom (Članovi 82 do 86, Zakona).

6. Smernice za poštenu obradu podataka o ličnosti

Podaci o ličnosti se u Školi moraju obrađivati samo kada su eksplicitno ovlašćeni od Lica za zaštitu podataka o ličnosti ili lica imenovanog za poslove zaštite podataka u Školi i odobreni od Direktora Škole kao rukovaoca podataka.

Škola mora da proceni i odluči da li da izvrši *Procenu uticaja obrade na zaštitu podataka – DPIA (Data Protection Impact Assessment)* za svaku aktivnost obrade u skladu sa smernicama (Član 54, Zakona).

6.1. Obaveštenje o privatnosti za fizička lica

U vreme skupljanja ili pre skupljanja podataka o ličnosti za svaku vrstu aktivnosti obrade, uključujući, ali se ne ograničavajući na kupovinu i prodaju roba, usluge ili markentiške aktivnosti, Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti je odgovorno da propisno obavesti lica na koje se podaci odnose o sledećem: *vrsti skupljenih podataka o ličnosti, namenama obrade, metodama obrade, pravima lica na koje se podaci odnose, periodu zadržavanja, potencijalnom međunarodnom prenosu podataka, deljenju podataka sa trećim stranama i merama Škole za zaštitu podataka o ličnosti*. Ove informacije se obezbeđuju kroz dokument Obaveštenje o privatnosti (*Privacy Notice*).

Ako Škola ima višestruke i različite aktivnosti obrade i obrađuje različite vrste podataka o ličnosti, treba izraditi različita Obaveštenja o privatnosti, zavisno od vrsta obrade podataka i kategorija podataka (na primer, jedno za namenu slanja poštom, a drugo za slanje špedicijom, gde se razlikuju aktivnosti obrade).

Ako se podaci o ličnosti dele sa trećom stranom, Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti Škole mora osigurati da je lice na koje se podaci odnose obavešteno o tome kroz Obaveštenje o privatnosti.

Kada se lični podaci prenose u treću zemlju prema *Politici prekograničnog prenosa* i Zakonu, u Obaveštenju o privatnosti treba jasno navesti državu u koju se podaci prenose i entitet kojem se podaci prenose.

6.2. Dobijanje pristanka

Kad god je obrada ličnih podataka zasnovana na pristanku fizičkog lica, ili na drugom zakonskom osnovu, *Lice za zaštitu podataka o ličnosti* ili lice imenovano za poslove zaštite podataka o ličnosti u Školi je odgovorno za evidentiranje i održavanje zapisa o tom pristanku, informisanje fizičkih lica, obezbeđivanje opcije za dostavljanje pristanka, i osiguranje da njihov pristanak (kad god se pristanak za obradu daje na zakonskoj osnovi) može biti u svako vreme povučen, na osnovu pisanog zahteva.

Kada se skupljaju podaci o deci ispod 15 godina starosti, *Lice za zaštitu podataka o ličnosti* ili lice imenovano za poslove zaštite podataka o ličnosti mora osigurati da roditelj (staralac) deteta, dobije *Formular za roditeljski pristanak* koji propisuje Nadzorno telo (Poverenik) (Član 16, Zakona). Rukovalac mora preduzeti razumne mere u cilju utvrđivanja da li je pristanak dao roditelj koji vrši roditeljsko pravo, odnosno drugi zakonski zastupnik maloletnog lica, uzimajući u obzir dostupne tehnologije.

Kada se zahteva korekcija, dopuna ili uništavanje zapisa podataka o ličnosti, *Lice za zaštitu podataka o ličnosti*, ili lice imenovano za poslove zaštite podataka o ličnosti osiguraće da se ovi zahtevi izvrše u razumnom vremenu, registruju i čuvaju logovi zapisa o zahtevima.

Podaci o ličnosti se obrađuju samo za namene za koje su originalno skupljeni. U slučaju da Škola želi obrađivati podatke za drugu namenu, Škola će tražiti eksplicitan pristanak od lica na koje se podaci odnose u jasnom i konciznom pisanom formatu. Svaki takav zahtev će uključivati originalnu namenu(e) za koju su se podaci skupljali, novu ili dodatnu namenu(e) obrade, kao i razlog za promenu namene(a) obrade. *Lice za zaštitu podataka o ličnosti* ili lice imenovano za poslove zaštite podataka o ličnosti u Školi odgovorno je za usaglašenost sa pravilima u ovoj sekciji.

Metod skupljanja podataka o ličnosti u Školi usaglašen je i biće usaglašavan ubuduće sa Zakonom o zaštiti podataka o ličnosti, dobrom praksom i standardima zaštite podataka i informacija.

7. Organizacija i odgovornosti

Odgovornost za osiguranje odgovarajuće obrade podataka o ličnosti je svakog ko radi za ili sa Školom i ima pristup podacima o ličnosti koje Škola obrađuje.

Ključne odgovornosti za obradu podataka o ličnosti u Školi imaju sledeće organizacione uloge:

Direktor: Odobrava opštu strategiju i donosi odluke o skupljanju, obradi i zaštiti podataka o ličnosti u Školi, radi kao rukovalac aktivnosti obrade, određuje namenu obrade, organizuje i vodi evidenciju o aktivnostima obrade podataka o ličnosti u Školi (Član 47(5) Zakona).

Lice za zaštitu podataka o ličnosti ili lice imenovano za poslove zaštite podataka o ličnosti: Odgovorno je za menadžment programa za zaštitu podataka o ličnosti, za razvoj i promociju politike zaštite privatnosti krajnjim korisnicima i za druge aktivnosti definisane u opisu poslova Lica za zaštitu podataka o ličnosti (Članovi 56, 57 i 58 Zakona);

Pravnik: Monitoriše i analizira zakone o zaštiti podataka o ličnosti, prati promene zakonskih regulativa, razvija zahteve za usaglašenost i pomaže sektorima Škole u dostizanju ciljeva *Politike zaštite privatnosti*.

IT sektor:

- Odgovoran je da osigura da svi sistemi, servisi i oprema koja se koristi za obradu i pohranjivanje podataka o ličnosti dostignu prihvatljive standarde informacione bezbednosti i zaštite podataka o ličnosti.
- Izvršava regularne provere i skeniranja da osigura da tehničke mere zaštite hardvera i softvera, i organizacione mere funkcionišu propisno.

Marketing sektor:

- Odgovoran je za odobravanje svakog saopštenja o zaštiti podataka o ličnosti koje se prilaže uz komunikaciona sredstva kao što su e-mail, faks poruke i pisma.
- Odgovara na svaki upitnik o zaštiti podataka od strane novinara ili drugih medija.
- Gde je neophodno, radi sa *Licem za zaštitu podataka o ličnosti* ili licem imenovanim za poslove zaštite podataka o ličnosti, da osigura marketing i da usaglasa inicijative za promociju **Škole** sa principima zaštite podataka.

8. Odgovor na incident povrede podataka o ličnosti

Kada Škola, tj. *Lice za zaštitu podataka o ličnosti* ili lice imenovano za poslove zaštite podataka o ličnosti, uoči ili posumnja, ili identifikuje incident stvarne povrede ličnih podataka, mora da preduzme internu proveru, spreči širenje incidenta i zahteva blagovremene mere oporavka sistema zaštite, u skladu sa ovom *Politikom*. Gde postoji rizik, posebno visok rizik za prava i slobode lica na koja se podaci odnose, Škola (tj. *Lice za zaštitu podataka o ličnosti* ili lice imenovano za poslove zaštite podataka o ličnosti) će obavestiti nadležno nadzorno telo

(Poverenika) i Nacionalni CERT bez odlaganja, a najkasnije u roku od 72 sata, a u najkraćem mogućem roku vlasnike podataka (do 15 dana).

9. Provera i odgovornost

Škola će nastojati da provera kvalitet implementacije ove Politike, da unapređuje tehnike i organizacione mere zaštite i kontrole podataka o ličnosti klijenata.

Svaki zaposleni u Školi, koji obrađuje podatke o ličnosti moraju biti upoznati i obučeni o podacima o ličnosti, o sistemima kontrole i načinu prikupljanja i obrade, zakonskim propisima i odgovornostima koje proizilaze iz Zakona. Ako zaposleni u Školi povredi prava i slobode lica na koje se podaci odnose, prema ovoj Politici, biće podvrgnut disciplinskim, prekršajnim ili krivičnim merama, zavisno od nanete štete poslovanju Škole.

10. Menadžment održavanja zapisa politike

Ime zapisa	Lokacija skladištenja	Lice odgovorno za skladištenje	Kontrole za zaštitu zapisa	Vreme čuvanja
<i>Formular pristanka vlasnika podataka</i>	(specifikovati folder u bazi podataka IKT sistema)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	10 godina
<i>Formular za povlačenje pristanka lica čiji se podaci obrađuju</i>	(specifikovati folder u bazi podataka IKT sistema)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	10 godina

<i>Formular za roditeljski pristanak</i>	(specifikovati folder u bazi podataka IKT sistema)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	10 godina
<i>Formular za povlačenje roditeljskog pristanka</i>	(specifikovati folder u bazi podataka IKT sistema)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	10 godina
<i>Ugovor o prenosu podataka o ličnostima</i>	(specifikovati folder u Intranetu Škole)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	5 godina od prestanka važnosti Sporazuma

<i>Registar obaveštenja o privatnosti</i>	(specifikovati folder u Intranetu Škole)	Lice za zaštitu podataka o ličnosti	Samo ovlašćeno lice može pristupiti formularu	Permanentno
---	--	-------------------------------------	---	-------------

11. Validacija i menadžment dokumenta

Validaciju ove politike vrše vlasnik (staratelj) ove politike, Lice za zaštitu podataka o ličnosti i Direktor koji mora kontrolisati i proveravati primenu politike o zaštiti privatnosti, a Lice za zaštitu podataka o ličnosti po potrebi i ažurirati dokument najmanje jedanput godišnje.

Ova politika stupa na snagu danom potpisivanja: 28.03.2023. godine

Direktor Škole

Prilog 1. TEHNIČKE I ORGANIZACIONE MERE ZAŠTITE AKTIVNOSTI OBRADE PODATAKA O LIČNOSTI

Zaštita poverljivosti aktivnosti obrade podataka o ličnosti	
<i>Obrada podataka</i>	<i>Kontrola zaštite aktivnosti obrade</i>
Fizički pristup prostorijama za obradu podataka	Ključevi, sistemi zaštite prostorija, i/ili obezbeđenje na ulazu, alarmni sistemi, video nadzor.
Elektronski pristup sistemima za obradu i pohranjivanje podataka	Bezbedna lozinka, mehanizam za automatsko blokiranje/zaključavanje, dvokratna autentifikacija, šifrovanje nosača podataka/medija za pohranjivanje.

Pristup fizičkog lica za čitanja, kopiranja, izmene ili brisanja podataka u IS Škole	Koncept autorizacije prava pristupa fizičkog lica na koje se podaci odnose IKT sistemu Škole na bazi potrebe i analize rizika događaja sistemskog pristupa i davanje pristupa uz manuelnu pomoć administratora sistema Škole.
Izolovana obrada podataka	Sistemi za podršku više klijenata.
Proces obrade podataka o ličnosti	Pseudonimizacija: Obrada podataka o ličnosti na takav način/metod da se podaci ne mogu povezati sa specifičnim licem bez pomoći dodatnih informacija, pod uslovom da su ove informacije skladištene odvojeno i predmet su odgovarajućih tehničkih i organizacioneih mera zaštite.
Zaštita integriteta aktivnosti obrade podataka o ličnosti	
Prenos podataka o ličnosti	Adekvatne tehničke mere zaštite koje uključuju šifrovanje, VPN veze, digitalni potpis za zaštitu od neovlašćenog čitanja, kopiranja i izmena ili brisanja podataka u prenosu.
Tačnosti unosa podataka o ličnosti	Kontrola logovanja i dokument menadžment sistema.
Zaštita raspoloživost i otpornosti ličnih podataka	
Kontrola raspoloživosti i sprečavanje slučajne ili namerne destrukcije ili gubitka podataka o ličnosti	Strategija bekapovanja (<i>online/offline; onsite/offsite</i>), UPS sitem, antivirusna zaštita, <i>firewwal</i> , procedura za izveštavanje i plan vanrednih događaja.

Brz oporavak posle incidenta	Iz sistema za bekapovanje, oporavak izbrisanih podataka alatima i tehnikama digitalne forenzike.
Organizacione mere zaštite	
Procedure za regularno testiranje, procenu i evaluaciju	
Menadžment zaštite privatnosti	Politika zaštite privatnosti, Registar aktivnosti obrade
Menadžment odgovora na incident	Politika upravljanja incidentom, Procedura prvog odgovora na incident
Podrazumevana i ugrađena zaštita podataka o ličnosti	<p>Implementirana <i>pseudonimizacija</i> i <i>minimizacija</i> vidljivosti podataka o ličnosti za implementaciju načela zaštite podataka o ličnosti, integracija neophodnih mera zaštite (ISMS, Zakon) u procese obrade.</p> <p>Ova kontrola se odnosi na količinu skupljanja podataka, obim obrade, period skladištenja i pristup podacima o ličnosti,</p> <p>Osigurati da podrazumevano podaci o ličnosti nisu dostupni fizičkim licima bez intervencije čoveka za neki neodređen broj lica koji traže pristup svojim podacima, pa je manuelna pomoć administratora neophodna.</p>