

Politika zaštite podataka*

Povijest dokumenta

<i>Školska ustanova*</i>	<i>Obrada*</i>
GOSPODARSKA ŠKOLA ISTITUTO PROFESSIONALE	sve obrade osobnih podataka
<i>Datum izrade</i>	<i>Službenik za zaštitu podataka*</i>
11. srpnja 2019.	William Bello
<i>Datum zadnje provjere</i>	<i>Tajnik</i>
04. veljače 2022.	LJILJANA RADULOVIĆ
<i>Datum slijedeće provjere</i>	<i>Odgovorna osoba / ravnatelj*</i>
04. veljače 2023.	MILIVOJ GOSPIĆ

Datum	Komentar	Autor
11.07.2019.	Izrada Politike i priloga	William Bello
11.07.2020.	Provjera Politike i priloga, manja usklađenja s EDPB i AZOP smjernicama Politika nije u punoj primjeni, najviše, kao posljedica Covid-19 situacije	William Bello
11.07.2021.	Provjera Politike i priloga, manja usklađenja s EDPB i AZOP smjernicama Politika nije u punoj primjeni, najviše, kao posljedica Covid-19 situacije	William Bello
04.02.2022.	Provjera Politike i priloga, manja usklađenja s EDPB i AZOP smjernicama Politika nije u punoj primjeni, najviše, kao posljedica Covid-19 situacije	William Bello

Važna napomena

Politika zaštite podataka (privatnosti) je interni dokument GOSPODARSKE ŠKOLE ISTITUTO PROFESSIONALE, BUJE kojim odgovorne osobe, prema Pravilniku o zaštiti podataka, upravljaju ciljevima, strategijom i aktivnostima održavanja sukladnosti s Općom uredbom o zaštiti podataka EU 2016/679.

Ovaj dokument je polazište za izradu daljnjih standarda, okvira, smjernica i procedura koje se koriste za zaštitu podataka a odvijaju se kroz aktivnosti programa zaštite podataka i treba biti usklađen sa stvarnim mogućnostima Škole.

Ovaj dokument se ažurira prema potrebi kako bi odrazio promjene u radu Škole, tehnologije, regulative i ostalih faktora koji utječu na obradu osobnih podataka.

Ovaj dokument je namijenjen svima koji su na bilo koji način uključeni u provođenje pojedinih aktivnosti unutar poslovnih procesa i očekuje se od njih da ga pročitaju i primjene u svom radu.

Ukoliko niste sigurni da kroz aktivnost koju planirate obrađujete zaista osobne podatke, tada pretpostavite da ih obrađujete i da se na vas primjenjuje ova Politika.

Nepridržavanje ili kršenje članaka iz ove Politike može imati ozbiljne posljedice po Školu, ali i pojedince jer predstavlja kršenje Pravilnika o zaštiti podataka, ugovora o radu i potpisanih Izjava o povjerljivosti te zakonski propisa i EU uredbi na području zaštite podataka, za što su predviđene disciplinske i novčane kazne.

Za sva pojašnjenja ili nedoumice u svezi primjene ove Politike i općenito zaštite podataka obratite se imenovanom Službeniku za zaštitu podataka: William Bello, email: dpo@bello.hr.

Sadržaj

1	UVOD	5
1.1	GOSPODARSKA ŠKOLA ISTITUTO PROFESSIONALE	POGREŠKA! KNJIŽNA OZNAKA NIJE DEFINIRANA.
1.2	POLITIKA ZAŠTITE PODATAKA (PRIVATNOSTI)	6
1.3	VIZIJA I MISIJA PROGRAMA ZAŠTITE PODATAKA	6
1.4	PODRUČJE ZAŠTITE PODATAKA	7
1.5	OKVIR ODVIJANJA ZAŠTITE PODATAKA	7
1.6	STRATEGIJA ZAŠTITE PODATAKA	8
1.7	AKTIVNOSTI ZAŠTITE PODATAKA - PROGRAM PRIVATNOSTI	8
1.8	MAPA OSOBNIH PODATAKA I REGISTAR OBRADA	8
2	PRIMJERENE TEHNIČKE I ORGANIZACIJSKE MJERE ZAŠTITE PODATAKA	9
2.1	PROCJENA UČINKA NA ZAŠTITU PODATAKA	9
2.2	PRAĆENJE ŽIVOTNOG CIKLUSA PODATKA	9
2.3	TEHNIČKA I INTEGRIRANA ZAŠTITA PODATAKA	9
2.4	EVIDENCIJA AKTIVNOSTI OBRADU PODATAKA	10
2.5	ANGAŽIRANJE IZVRŠITELJA OBRADU	10
3	ZAŠTITA PODATAKA U OBRADAMA OSOBNIH PODATAKA	10
3.1	OSNOVNO POSLOVANJE ŠKOLE	10
3.2	PODRŠKA POSLOVANJU ŠKOLE	11
3.3	PRIKUPLJANJE, KORIŠTENJE, PROSLJEĐIVANJE, POHRANA I BRISANJE PODATAKA	11
3.3.1	PRAVNE OSNOVE ZA OBRADU OSOBNIH PODATAKA	11
3.3.2	KORIŠTENJE PODATAKA U OBRADAMA	12
3.3.3	PROSLJEĐIVANJE PODATAKA	12
3.3.4	POHRANA PODATAKA	12
3.3.5	BRISANJE PODATAKA	13
4	KODEKS PONAŠANJA	13
5	PRILOZI	13
5.1	STRATEGIJE I TAKTIKE PRIPREME ZA OBRADU OSOBNIH PODATAKA	13
5.1.1	MINIMIZACIJA PODATAKA (MINIMISE)	13
5.1.2	ODVAJANJE PODATAKA (SEPARATE)	13
5.1.3	APSTRAKCIJA PODATAKA (ABSTRACT)	14
5.1.4	SKRIVANJE PODATAKA (HIDE)	14
5.1.5	INFORMIRANJE	14
5.1.6	KONTROLA	14
5.1.7	PROVOĐENJE	14

5.1.8	DOKAZIVANJE	15
5.2	WB PRIVACY PROGRAM MANAGER INTERNET PORTAL	15
5.2.1	PROGRAM PRIVATNOSTI	15
5.2.2	OKVIR ZA UPRAVLJANJE RIZICIMA	15
5.2.3	OBRADA ZAHTJEVA ISPITANIKA	15
5.2.4	PRAĆENJE INCIDENTA I POVREDE PODATAKA	15
5.2.5	OKVIR PROGRAMA	15
5.2.6	DOKAZIVANJE POUZDANOSTI	16
5.2.7	REGISTAR OBRADA I PODATAKA	16
5.2.8	SUDIONICI PROGRAMA PRIVATNOSTI	16
5.2.9	OBRADA PODATAKA	16
5.2.10	PRIENOS PODATAKA	16
5.2.11	ARHITEKTURA POSLOVNOG SUSTAVA	16
5.3	PREGLED OBRADA KOJE PROVODI ŠKOLA	17
5.3.1	OBRADE U SVRHU PROVOĐENJA ODGOJNIH I OBRAZOVNIH AKTIVNOSTI	17
5.3.2	OBRADE ZA PODRŠKU RADA ŠKOLE	17
5.4	KLASIFIKACIJA OSOBNIH PODATAKA	17
5.4.1	VANJSKI	17
5.4.2	SOCIJALNI	17
5.4.3	INTERNI	17
5.4.4	PRAĆENJE	17
5.4.5	ODGOJNI	17
5.4.6	EDUKATIVNI	17
5.4.7	FINANCIJSKI	17
5.4.8	POVIJESNI	17
5.4.9	ŠKOLSKI PODACI	18

1 Uvod

1.1 GOSPODARSKA ŠKOLA ISTITUTO PROFESSIONALE

1.2 **Gospodarska škola Istituto professionale, Buje (u nastavku: Škola) javna je ustanova koja obavlja djelatnost odgoja i obrazovanja u svojstvu srednje škole, sukladno Zakonu o odgoju i obrazovanju u osnovnoj i srednjoj školi.**

Osnivač Škole je Istarska županija

OIB Škole je 27648687825.

Svoju djelatnost Škola obavlja na lokaciji: Buje, Školski brijeg 1

Komunikacija s djelatnicima Škole ostvariva je putem slijedećih komunikacijskih kanala:

Poštom na adresu: 52460 Buje, Školski brijeg 1

Telefon: 052 492772

Elektronička pošta: skola@ss-gospodarska-buje.skole.hr

Djelatnost srednjeg obrazovanja u srednjim školama obuhvaća opće obrazovanje i različite vrste i oblike obrazovanja, osposobljavanja i usavršavanja koji se ostvaruju u skladu s odredbama Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi i zakona kojima se uređuju djelatnosti pojedinih vrsta srednjih škola.

Djelatnost obrazovanja odraslih osoba ostvaruje se u skladu s odredbama Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi i posebnog zakona.

Poslovanje Škole uređeno je važećim zakonima Republike Hrvatske i uredbe EU, te uz ostale ovi zakonski propisi, pravilnici koji iz njih proizlaze i ostali obvezujući akti utječu na obradu osobnih podataka:

- Zakon o radu
- Zakon o obveznim odnosima
- Zakon o mirovinskom osiguranju
- Zakon o zdravstvenoj zaštiti
- Zakon o dobrovoljnom zdravstvenom osiguranju
- Zakon o doprinosima
- Zakon o knjižnicama
- Zakon o pravu na pristup informacijama
- Zakon o računovodstvu
- Zakon o strukovnom obrazovanju
- Zakon o zaštiti na radu
- Obiteljski zakon
- Opći porezni zakon
- Zakon o arhivskom gradivu i arhivima
- Zakon o obrazovanju odraslih
- I drugi

Posebno:

- Opća uredba o zaštiti podataka EU 2016/679
- Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/18
- Zakon o elektroničkim medijima
- Zakon o informacijskoj sigurnosti

Pravni akti Škole koji uređuju i utječu na zaštitu podataka su:

- Pravilnik o zaštiti podataka
- Pravilnik o arhivskom građu
- Pravilnik o informacijskoj sigurnosti

Prilikom zapošljavanja i sklapanja ugovora o radu zaposlenik potpisuje Izjavu o povjerljivosti kojom prihvaća obveze čuvanja poslovne tajne i obvezu zaštite podataka ispitanika čije osobne podatke prikuplja i obrađuje Škola.

Škola zapošljava manje od 50 osoba.

1.3 Politika zaštite podataka (privatnosti)

Politika zaštite podataka (privatnosti) je interni dokument Gospodarske škole Istituto professionale, Buje kojim odgovorne osobe, prema Pravilniku o zaštiti podataka, upravljaju ciljevima, strategijom i aktivnostima održavanja sukladnosti s Općom uredbom o zaštiti podataka EU 2016/679.

Ovaj dokument je polazište za izradu daljnjih standarda, okvira, smjernica i procedura koje se koriste za zaštitu podataka a odvijaju se kroz aktivnosti programa zaštite podataka i treba biti usklađen sa stvarnim mogućnostima Škole.

Ovaj dokument se ažurira prema potrebi kako bi odrazio promjene u radu Škole, tehnologije, regulative i ostalih faktora koji utječu na obradu osobnih podataka.

Ovaj dokument je namijenjen svima koji su na bilo koji način uključeni u provođenje pojedinih aktivnosti unutar poslovnih procesa i očekuje se od njih da ga pročitaju i primjene u svom radu.

Ukoliko niste sigurni da kroz aktivnost koju planirate obrađujete zaista osobne podatke, tada pretpostavite da ih obrađujete i da se na vas primjenjuje ova Politika.

Nepridržavanje ili kršenje članaka iz ove Politike može imati ozbiljne posljedice po Školu, ali i pojedince jer predstavlja kršenje Pravilnika o zaštiti podataka, ugovora o radu i potpisanih Izjava o povjerljivosti te zakonski propisa i EU uredbi na području zaštite podataka, za što su predviđene disciplinske i novčane kazne.

Za sva pojašnjenja ili nedoumice u svezi primjene ove Politike i općenito zaštite podataka obratite se imenovanom Službeniku za zaštitu podataka: William Bello, email: dpo@bello.hr.

Zadatak je odgovorne osobe da upozna i organizira djelotvorno i redovno upoznavanje djelatnika s njenim sadržajem, kao i da osigura njezinu redovnu provjeru ažurnosti i svrhovitosti. Također, odgovorna osoba mora osigurati sve preduvjete i potrebne resurse (vrijeme, aplikacije, edukaciju i sl.) za djelovanje grupe za zaštitu podataka a posebno službenika za zaštitu podataka.

Zadatak je službenika za zaštitu podataka da najmanje jednom godišnje procijeni koliko se ova Politika primjenjuje u praksi te da predloži korekcije i poboljšanja.

Ukoliko niste sigurni da kroz aktivnost koju planirate obrađujete zaista osobne podatke, tada pretpostavite da ih obrađujete i da se na vas primjenjuje ova Politika.

Nepridržavanje ili kršenje članaka iz ove Politike može imati ozbiljne posljedice po Školu, ali i pojedince jer predstavlja kršenje ugovora o radu i potpisanih Izjava o povjerljivosti.

Sve zainteresirane strane su svjesne da se ovaj dokument razvija tijekom vremena prateći promjene u radu Škole, nova saznanja na području zaštite podataka, razvoj novih tehnologija obrade podataka kao i zakonske regulative i prakse na području zaštite podataka.

1.4 Vizija i misija programa zaštite podataka

U obavljanju svojih zadaća kao odgojna i obrazovna ustanova, ostalih poslovnih aktivnosti, odnosu s učenicima, roditeljima i skrbnicima, zaposlenicima, posjetiteljima i prilikom korištenja usluga svojih dobavljača <naziv škole> promiče i poštuje informacijsku privatnost i provodi zaštitu osobnih podataka poštujući principe i načela Opće uredbi o zaštiti podataka EU 2016/679.

U ostvarenju zaštite podataka, Škola najmanje:

- osigurava da svaku obradu osobnih podataka provodi poštujući principe iz Članka 5. GDPR, a posebno,
- da za obradu ima opravdanu pravnu osnovu sukladno Članku 6.1 GDPR, te da
- informira ispitanika o podacima i svrsi prikupljanja sukladno Članku 13 i 14, kao i da se
- pridržava dozvoljenih okvira dijeljenja podataka, te da
- poštuje prava pojedinca, pri čemu
- provodi mjere informacijske sigurnosti nad osobnim podacima

1.5 Područje zaštite podataka

Škola na svojoj lokaciji prikuplja i obrađuje osobne podatke polaznika edukativnih aktivnosti i njihovih roditelja i li skrbnika u svojstvu voditelja obrade.

U svrhu realizacije ugovora o radu, Škola prikuplja i obrađuje osobne podatke zaposlenika prilikom zapošljavanja i prema potrebi kontinuirano tijekom rada.

Osobne podatke prosljeđuje trećim stranama isključivo temeljem svoje zakonske obaveze sukladno zakonima RH na području rada, mirovinskog i zdravstvenog osiguranja te ostalih pozitivnih zakonskih propisa koji uređuju odnose poslodavca i posloprimca te ugovornih obveza.

Osobni podaci se ne prenose u treće zemlje (van EEA).

Strukturirani i nestrukturirani osobni podaci pohranjeni su na IT sustavima CARNET i na računalima na lokaciji.

Pohranjeni podaci obrađuju se, čuvaju i prenose sukladno politici informacijske sigurnosti i zaštićeni odgovarajućim organizacijskim i tehničkim mjerama Škole i CARNET.

Podaci se čuvaju samo onoliko dugo koliko je to potrebno za njihovu obradu sukladno zakonskim propisima za pojedine obrade i Pravilniku o arhivskoj građi Škole, nakon čega se, brišu, uništavaju ili zasebno arhiviraju ukoliko imaju doživotni period trajanja.

Škola upravlja svojim javnim Internet portalom na adresi: www.ss-gospodarska-buje.skole.hr.

Škola ne prikuplja direktno ili indirektno osobne podatke u svrhu analitike korištenja web stranica.

Školska ustanova na svojim javnim web stranicama koristi isključivo web „kolačiće“ koji su tehnički neophodni za odvijanje komunikacije između korisnikove terminalne opreme i Internet mjesta na kojemu se nalazi web stranica Škole te pružanje usluge na Internet mjestu web stranice Škole na zahtjev korisnika odabirom nekog od ponuđenih sadržaja (primjerice dohvat objavljenih dokumenata).

1.6 Okvir odvijanja zaštite podataka

U svrhu ispunjenja svoje misije zaštite podataka, Škola je procijenila rizike koji se mogu pojaviti prilikom obrade osobnih podataka te je u cilju postavljanja kontrola kojima se prepoznati rizici smanjuju postavila okvir aktivnosti unutar kojega se odvija program informacijske privatnosti i zaštite osobnih podataka (kraće: "program privatnosti ili zaštite podataka").

Provođenjem programa privatnosti Škola ispunjava obavezu u smislu Članka 5. stavak 2 GDPR. Prikupljanjem rezultata pojedine izvršene aktivnosti, Škola kao voditelj obrade time osigurava dokaze svoje usklađenosti (pouzdanost) sa Člankom 5. stavak 1.

Program privatnosti Škole usklađen je s tehničkim i organizacijskim mjerama zaštite.

Kao osnovni model i polazište za analizu rizika povrede privatnosti, Škola koristi Opću uredbu o zaštiti podataka EU 2016/679 i Zakon o provedbi Opće uredbe NN 42/18.

Okvir programa privatnosti zasnovan je na globalno priznatom okviru upravljanja programom privatnosti (Privacy Management Activity Framework) kanadske tvrtke Nymity implementiranom na Podio platformi tvrtke Citrix pod zaštićenim nazivom „WB Privacy Program Manager“ (WB-PPM). Prilikom usvajanja okvira u kojemu se odvija program privatnosti konzultirana je dobra praksa, korišteni su prihvaćeni standardi i norme poput ISO27001, ISO27002, ISO27701 i preporuke nadzornih tijela EDPB, CNIL FR, ICO UK i AZOP HR.

1.7 Strategija zaštite podataka

Grupno osoba koje su posebno zadužene za zaštitu osobnih podataka čine:

- (1) ravnatelj
- (2) tajnik
- (3) voditelj računovodstva
- (4) administrator informatičke potpore
- (5) službenik za zaštitu podataka

Administrator informatičke potpore je osoba odgovorna za sva pitanja informacijske sigurnosti odgovorna za sva pitanja informacijske zaštite podataka i po tom pitanju izvještava direktno ravnatelja, prema potrebi odnosno barem jednom godišnje. Ukoliko administrator informatičke potpore ima neka otvorena pitanja iz područja primjene informacijske sigurnosti na zaštitu podataka o tome se savjetuje sa službenikom za zaštitu podataka.

Najmanje jednom godišnje Škola će provesti program osvještavanja za sve zaposlene i obuke za članove grupe za zaštitu podataka.

Najmanje jednom godišnje, Škola će provesti internu procjenu usklađenosti s GDPR i provođenja redovnih aktivnosti programa privatnosti.

1.8 Aktivnosti zaštite podataka - program privatnosti

Aktivnosti programa privatnosti grupirane su u slijedeće kategorije:

- (1) Uspostaviti sustav upravljanja
- (2) Ažurirati popise osobnih podataka
- (3) Usklađivati politike zaštite privatnosti
- (4) Ugraditi zaštitu privatnosti podataka u svakodnevno poslovanje
- (5) Provoditi program obuke i osvještavanja
- (6) Upravljanje rizicima informacijske sigurnosti
- (7) Upravljanje rizicima od treće strane
- (8) Održavati obavijesti
- (9) Odgovoriti na upite i pritužbe pojedinaca
- (10) Pratiti promjene ili novosti u poslovanju
- (11) Provoditi program upravljanja povredama privatnosti
- (12) Pratiti kako se barata podacima u stvarnosti
- (13) Biti u toku s događanjima na području zaštite podataka

Odgovorna osoba Škole osigurati će potrebne resurse kako bi se aktivnosti planirale te odvijale prema planu i u dogovorenom opsegu.

Aktivnosti unutar pojedinih kategorija izrađivati će se primjereno uvjetima, prema njihovoj hitnosti i u skladu s mogućnostima Škole.

1.9 Mapa osobnih podataka i registar obrada

Kako bi osigurala zaštitu pojedinaca prilikom obrade osobnih podataka, Škola evidentira svaki sustav koji prikuplja i obrađuje osobne podatke, bilo da je to ručna obrada korištenjem papirnate dokumentacije ili elektronička obrada podataka korištenjem informatičkih resursa.

Svaki suradnik u odgojno obrazovnom procesu kao i oni koji sudjeluju u ostalim aktivnostima koje podržavaju poslovanje Škole moraju biti svjesni da trebaju prijaviti Službeniku za zaštitu podataka svaki takav sustav koji oni koriste za svoje polaznike obrazovanja, nastavnike, radnike ili druge fizičke osobe. Nužno je evidentirati koji osobni podaci se prikupljaju, bilo da su to jaki identifikatori ili osjetljivi podaci o pojedincima ili se uz određene metode ti podaci mogu koristiti kako bi se nekoga identificiralo, te time nastupa mogućnost zloupotrebe.

Potrebno je evidentirati IT infrastrukturu i korištene resurse kao i prijenos podataka između pojedinih sustava, te mjesta njihovog zadržavanja nakon obrade (mirovanje).

Potrebno je izraditi mapu podataka koja pokazuje gdje se ti podaci nalaze, koje resurse koriste, način i uvjete prelaza između sustava, organizacija i lokacija.

Potrebno je izraditi i kasnije obavezno primjenjivati klasifikaciju osobnih podataka. Polazni primjer te klasifikacije nalazi se u Prilogu Klasifikacija osobnih podataka.

Planirano je da se mapa osobnih podataka i registar obrada zajedno sa sustavima evidentira i dokumentira u WM-PPM alatu.

2 Primjerene tehničke i organizacijske mjere zaštite podataka

Provođenje mjera kontrole rizika koji su propisani kroz Pravilnik o informacijskoj sigurnosti te slijedom njega Politiku informacijske sigurnosti s pratećim standardima i uputama nužni je preduvjet učinkovitog provođenja zaštite osobnih podataka ali nije dovoljno.

Škola je obvezna prilikom obrade osobnih podataka provoditi primjerene tehničke i organizacijske mjere u cilju osiguranja dovoljnoga nivoa zaštite podataka i sprečavanja njihove zloupotrebe ili neovlaštenog preuzimanja.

Prilikom planiranja i provođenja tehničkih i organizacijskih mjera zaštite podataka obavezno je uključiti službenika za zaštitu podataka u što ranijoj fazi planiranja i pripreme. Službenik za zaštitu podataka u obavezi je da redovno provjerava provođenje planiranih tehničkih i organizacijskih mjera.

U daljem su navedene neke od tih mjera.

2.1 Procjena učinka na zaštitu podataka

Prilikom određivanja svrhe i načina obrade osobnih podataka zadužena osoba obavezna je procijeniti visinu učinka obrade na zaštitu podataka prilikom samog početka nove obrade ili izmjene postojeće iz bilo kojeg razloga.

Pri tome ukoliko se procjeni da postoji mogućnost povrede podataka ili se sa sigurnošću to ne može otkloniti obavezno se mora zatražiti mišljenje službenika za zaštitu podataka.

Rezultati procjene se moraju dokumentirati. U Prilogu WB Privacy Program Manager Internet portal nalazi se opis sustava dokumentiranja koji je na raspolaganju članovima grupe za zaštitu podataka.

2.2 Praćenje životnog ciklusa podatka

Kada se započinje planiranje nove obrade ili se radi izmjena postojeće, obavezno se razmatra i dokumentira u svakoj fazi razvoja tijekom analize učinka i potrebnih mjera zaštite u svakom koraku životnog ciklusa podatka:

- (1) Prikupljanje
- (2) Korištenje
- (3) Prosljeđivanje
- (4) Zadržavanje
- (5) Uništavanje

Službenik za zaštitu podataka obavezan je pružiti svaku pomoć i savjet prilikom analize životnog ciklusa podatka.

2.3 Tehnička i integrirana zaštita podataka

Tehnička i integrirana zaštita podataka¹ (kraće PbD/D) provodi se svaki puta kao osnovna i zadana aktivnost zaštite podataka kojom se osigurava postizanje najviše sigurnosti i u najvećoj mjeri otklanjanju mogućnosti zloupotrebe podataka, u cilju sprečavanja povrede privatnosti ispitanika.

¹ Eng. Privacy by design by Default

Prilog ove Politike „Strategije i taktike pripreme za obradu osobnih podataka“ sadrži opis dokumentirane dobre prakse provođenja tehničke i integrirane zaštite podataka.

U prvim fazama planiranja i pripreme aktivnosti koje prikupljaju i obrađuju osobne podatke obavezno se treba konzultirati sa službenikom za zaštitu podataka.

2.4 Evidencija aktivnosti obrade podataka

Škola vodi računa o svim obradama osobnih podataka nastojeći prepoznati i umanjiti rizike koji mogu pri tome naškoditi pojedincima, a posebno uzimajući u obzir činjenicu da glavnu kategoriju ispitanika čine djeca.

Posebno se evidentiraju one obrade osobnih podataka za koje je utvrđeno procjenom učinka da će vjerojatno prouzročiti visok rizik za prava i slobode ispitanika, koje nisu povremene ili obrada uključuje posebne kategorije podataka iz članka 9. stavka 1. GDPR ili je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima iz članka 10. GDPR.

Prilikom procjene je li potrebno voditi evidenciju aktivnosti obrade podataka obavezno se treba konzultirati sa službenikom za zaštitu podataka.

2.5 Angažiranje izvršitelja obrade

Škola prilikom provođenja određene obrade osobnih podataka može angažirati drugu tvrtku da u njeno ime provodi tu obradu – izvršitelja obrade.

Škola će osigurati da se s organizacijom koja provodi obradu u njezino ime sklopi ugovor o obradi podataka te s istim upoznati službenika za zaštitu podataka. Prije sklapanja ugovora, odgovorna osoba Škole će utvrditi je li organizacija u dovoljnoj mjeri jamči provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz GDPR i da se njima osigurava zaštita prava ispitanika.

Škola će najmanje jednom godišnje provesti provjeru poštuje li izvršitelj obrade ugovor o obradi podataka.

3 Zaštita podataka u obradama osobnih podataka

3.1 Osnovno poslovanje Škole

Osnovno poslovanje² Škole usmjereno je na provođenje aktivnosti koje slijede iz prihvaćenog Kurikula i Plana programa i aktivnosti Škole na području odgoja i obrazovanja, što je primarna zadaća Škole kao javne obrazovne ustanove.

U sklopu osnovnog poslovanja ističu se ključne aktivnosti kroz koje se prikupljaju i obrađuju osobni podaci polaznika odgojnog i obrazovnog procesa, nastavnika, ostalih osoba uključenih u odgojno obrazovni proces, roditelja i skrbnika polaznika te ostalih osoba koje su direktno ili indirektno uključene u te aktivnosti.

Slijedeće svrhe obrade osobnih podataka podupiru ključne aktivnosti Škole u odgojno obrazovnom procesu (nije potpuna lista):

- Prijem i upis polaznika
- Praćenje i odvijanje odgojno-obrazovnih aktivnosti
- Izdavanje završnih dokumenata i ispis polaznika

Ostale aktivnosti (nije potpuna lista):

- Planiranje, organiziranje i upravljanje tijekom odgojno-obrazovnih aktivnosti iz kurikula Škole
- Planiranje, organiziranje i upravljanje tijekom drugih obrazovnih aktivnosti Škole
- Provođenje van-nastavnih aktivnosti
- Sudjelovanje u EU projektima

² Eng. „core business“

3.2 Podrška poslovanju Škole

Ključne grupe aktivnosti koje podupiru odvijanje poslovanja Škole (nije potpuna lista):

- Upravljanje ljudskim resursima (HR)
- Zaštita osoba i imovine
- Računovodstveno – financijski poslovi
- Informacijsko tehnološka podrška (IT)

Slijedeće svrhe obrade osobnih podataka podupiru odvijanje poslovanja Škole (nije potpuna lista):

- Zasnivanje radnog odnosa i promjene
- Redovni obračun i isplata plaća
- Obračun bolovanja i odsutnosti
- Praćenje preventivnih mjera zdravstvene zaštite
- Stručno usavršavanje i osposobljavanje djelatnika
- Zaštita osoba i imovine putem video nadzora
- Dodjeljivanje prava pristupa IT resursima

3.3 Prikupljanje, korištenje, prosljeđivanje, pohrana i brisanje podataka

Škola prikuplja osobne podatke ispitanika samo u određenu svrhu i samo ukoliko za to ima pravnu osnovu.

3.3.1 Pravne osnove za obradu osobnih podataka

Obrada osobnih podataka čiju svrhu određuje Škola zakonita je samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;

Obrada osobnih podataka u svrhu koja u najvećoj mjeri počiva na odlučivanju pojedinca, drugim riječima kada provedeni test ravnoteže između prava Škole i prava pojedinca prevagne u korist pojedinca, takva obrada se može provesti samo onda kada Škola dobije privolu pojedinca (ispitanika) za prikupljanje i obradu njegovih osobnih podataka u tu, određenu svrhu. Privola će u tom slučaju biti napisana jasnim i jednostavnim jezikom, uz isticanje prava pojedinca da povuče privolu, te će se ista pohraniti i čuvati kako bi se mogla dokazati zakonitost te obrade.

Škola većinu svojih obrada provodi jer je na to obvezna po ugovoru s ispitanikom, zakonu, ili ispunjavajući svoju javnu ulogu, a u nekim obradama i na osnovu legitimnog interesa. U rijetkim situacijama za obradu će jedina zakonita osnova biti privola.

Primjer je objava fotografija ili video snimki učesnika nastavnih aktivnosti na javnim web portalima, mrežnim stranicama ili službenim stranicama Škole ili obrada posebnih kategorija osobnih podataka (poput zdravstvenih podataka) u cilju organiziranja nastave u posebnim situacijama (poput Covid-19 pandemije).

b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;

Ugovor o radu, ugovor o smještaju u učenički dom, ugovor o obrazovanju ili pohađanju pojedinih edukacijskih aktivnosti van redovnog školovanja su primjeri takvih obrada. Podnošenje molbi za posao, prikupljanje i obrada tih osobnih podataka dio je radnji koje se provode na zahtjev ispitanika prije sklapanja ugovora.

c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade;

Škola kao javna ustanova dužna je poštovati zakonske odredbe i poslovati u skladu s pozitivnim zakonskim propisima Republike Hrvatske. Prikupljanje i obrada osobnih podataka kao i njihovo eventualno prosljeđivanje nadležnim tijelima po slovu zakona nužni su radi poštovanja pravnih obveza Škole.

Primjer su svi podaci koji su vezani s mirovinskim i zdravstvenim sustavom, Ministarstvom obrazovanja ili lokalnim nadređenim institucijama i slično.

d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe;

U pojedinim situacijama kada su ugroženi životi ili zdravlje ispitanika, primjerice nezgoda ili ozljeda koja zahtijeva hitnu intervenciju i prosljeđivanje ili prikupljanje određenih podataka o unesrećenoj osobi.

e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;

U pravilu sve obrade koje imaju za cilj provođenje odgojno obrazovnih aktivnosti Škole prema njenim pravnim aktima, prihvaćenom kurikulumu škole, planu i programu nastave provode se u cilju izvršavanja zadaće od javnog interesa. Redovni upisi u školu, pohađanje nastave, praćenje i izvještavanje s nastavnih aktivnosti pa do ispisa iz škole.

f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Kada Škola kao organizacija treba omogućiti svoj rad i osigurati potrebne preduvjete za provođenje svojih planova tada postoji legitimni interes za obradu osobnih podataka, ukoliko to ne ugrožava ili na neki način uskraćuje prava na privatnost ispitanika.

U cilju zaštite osoba i imovine, Škola može provoditi video nadzor određenih prostora u skladu sa zakonima koji reguliraju taj vid nadzora i zaštite.

Prilikom određivanja zakonitosti pojedine obrade, obavezno će se konzultirati službenik za zaštitu podataka.

3.3.2 Korištenje podataka u obradama

Osobni podaci se koriste u obradama isključivo u svrhu u koju su prikupljeni. Za svako drugo korištenje zatražit će se mišljenje Službenika za zaštitu podataka.

Prilikom svakog korištenja podataka za pojedinu svrhu uzima se u obzir princip minimizacije podataka te se koriste samo neophodni podaci za obradu.

3.3.3 Prosljeđivanje podataka

Škola prosljeđuje podatke isključivo onim organizacijama za koje ima zakonsku obvezu ili je to u skladu s pravnom osnovom obrade podataka.

Prilikom svakog prosljeđivanja podataka uzima se u obzir princip minimizacije podataka te se prosljeđuju samo neophodni podaci za tu svrhu.

3.3.4 Pohrana podataka

Škola je donijela Pravilnik o arhivskom građu temeljem kojega se određuje vrijeme pohrane podataka nakon prestanka njihove aktivnog korištenja u svrhe za koje su i prikupljeni.

Škola provodi redovne procedure provjere pohranjenih podataka te ih po isteku vremena pohrane uklanja na odgovarajući način: pohranom u propisane arhive na daljnje čuvanje ili brisanjem tj. uništavanjem. Ove postupke Škola provodi najmanje jednom godišnje na prelazu školske godine.

Djelatnici koji provode pojedine obrade posebno u nastavi, tajništvu, računovodstvu i IT podršci odgovorni su za pohranu tih podataka na način koji odgovara tehničkim i organizacijskim mjerama zaštite podataka kao i Pravilniku o informacijskoj sigurnosti.

Prilikom planiranja obrade uzima se u obzir i moguća različita vremena pohrane pojedinih kategorija podataka te se prema tome dizajnira i tehnička podrška obrade. Primjer je čuvanje podataka o zaposlenicima i učenicima na odvojenim mjestima u odnosu na kategoriju podataka i njihovo vrijeme pohrane.

3.3.5 Brisanje podataka

Brisanje i uništavanje podataka provodi se u razumnom roku nakon isteka vremena pohrane na pouzdani način.

Papirnati dokumenti uništavaju se u rezačima papira. Fizički mediji koji se ne mogu izbrisati uništavaju se na način koji onemogućuje svako poništavanje postupka i vraćanje sadržaja.

Elektronički zapisi se brišu (delete) i nakon brisanja se provodi aktivnost sistemskog brisanja (purge) obrisanih podataka.

4 Kodeks ponašanja

Škola primjenjuje neformalni samo-određujući Kodeks ponašanja za osnovne i srednje škole i učeničke domove izdano od strane Bello Consulting, koji se provodi kroz sustav „WB Privacy Program Manager“ (WB-PPM) a koristi Citrix Podio platformu.

Kontinuirana primjena Politike zaštite podataka korištenjem WB-PPM smatra se prihvaćanjem i provođenjem Kodeksa pouzdanosti zaštite podataka za osnovne i srednje škole i učeničke domove.

Škola provodi organizacijske i tehničke mjere kojima uklanja ili smanjuje rizik povrede osobnih podataka ispitanika čije osobne podatke prikuplja ili obrađuje u pojedinim aktivnostima svojih poslovnih aktivnosti.

Provodeći program zaštite podataka, Škola je uspostavila glavne okvire internih kontrola, posebno:

- stalne kontrole rizika od kršenja GDPR
- redovne kontrole koje provodi službenik za zaštitu podataka
- povremene kontrole koje nastupaju prilikom ad-hoc provjere nadzornog tijela

Aktivnosti programa zaštite podataka Škola usklađuje s preporukama, smjernicama i odlukama EDPB u cilju postizanja certifikacije kada se za to steknu uvjeti.

5 Prilozi

5.1 Strategije i taktike pripreme za obradu osobnih podataka

Škola Privacy by Design by Default provodi primjenom ovih strategija podijeljenih u dvije kategorije³:

1. Podatkovno orijentirane strategije (Data Oriented Strategies)

Prilikom utvrđivanja opsega osobnih podataka koji će se prikupljati i obrađivati, pored sagledavanja životnog ciklusa podatka, obavezno će se primijeniti slijedeće strategije i razmotriti mogućnost korištenja pojedinih taktika

5.1.1 Minimizacija podataka (Minimise)

Škola će odrediti najmanji mogući broj podataka koje treba prikupljati i obrađivati.

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Odabir (select) – odabrati samo zaista potrebne podatke
- Izdvajanje (exclude) – izdvojiti prilikom obrade nepotrebne podatke
- Odvajanje (strip) – odvojiti podatke koji više nisu potrebni u obradi
- Brisanje (destroy) – izbrisati podatke koji više nisu potrebni

5.1.2 Odvajanje podataka (Separate)

Prilikom dizajna obrade a posebno pohrane podataka Škola će razdvojiti logički ili fizičke podatke u najvećoj mogućoj mjeri

³ Prema Privacy Design Strategies (The Little Blue Book), Jaap-Henk Hoepman

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Izolirati (isolate) – izolirati podatke u zasebne baze ili poslužitelje
- Distribuirati (distribute) – razmjestiti obrade na zasebne fizičke lokacije

5.1.3 Apstrakcija podataka (Abstract)

Škola će ograničiti u najvećoj mogućoj mjeri detalje i prepoznavanje samih podataka koji se obrađuju

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Uopćavanje (summarise) – npr. umjesto datuma rođenja koristiti godinu starosti
- Grupiranje (group) – agregiranje podataka kako bi se obradila općenita informacija grupiranih podataka
- Izmjena (perturb) – koristiti u obradi izmijenjeni podatak kako bi se prikrila njegova prava vrijednost ili značenje

5.1.4 Skrivanje podataka (Hide)

Škola će zaštititi osobne podatke na način da ih se ne može povezati s osobom (deidentifikacija) kao i da se ne objave javno ili na drugi način povežu s osobom (reidentifikacija).

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Ograničiti (restrict) – provesti mjere kontrole pristupa podacima
- Prikriti (obfuscate) – prikriti značenje podataka, npr. maskiranje na snimkama
- Odvojiti (dissociate) – ukloniti jake identifikatore koji povezuju podatke s osobom
- Izmiješati (mix) – miješanje podataka kako bi se prikrio pravi identitet, anonimizacija

2. Procesno orijentirane strategije (Process Oriented Strategies)

Prilikom utvrđivanja opsega osobnih podataka koji će se prikupljati i obrađivati, potrebno je urediti procese, procedure, upute i informacije o zaštiti podataka, obavezno će se primijeniti slijedeće strategije i razmotriti mogućnost korištenja pojedinih taktika

5.1.5 Informiranje

Škola će pružiti informaciju ispitaniku o samoj obradi na vrijeme i na odgovarajući način.

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Objava (supply) – objaviti ispitaniku sve relevantne informacije o obradi osobnih podataka kroz Izjavu o zaštiti podataka (Privacy notice)
- Objašnjenje (explain) -objasniti ispitaniku razloge i detalje obrade osobnih podataka
- Obavijest (notify) – pružiti informaciju o obradi ispitaniku u trenutku kada se od njega prikupljaju osobni podaci

5.1.6 Kontrola

Škola će omogućiti ispitaniku odgovarajuću kontrolu nad obradom njegovih osobnih podataka

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Privola (consent) – osigurati da ispitanik da privolu za obradu svojih osobnih podataka kada za to nema druge pravne osnove
- Izbor (choose) – pružiti ispitaniku pravi izbor u odlučivanju hoće li pristati na obradu svojih osobnih podataka
- Ažuriranje (update) – omogućiti ispitaniku ažuriranje i održavanje svojih osobnih podataka
- Povlačenje (retract) – poštovati koliko je god to moguće zahtjev ispitanika za brisanjem podataka

5.1.7 Provođenje

Škola je odlučna u obradi podataka na način koji štiti podatke i privatnost ispitanika te će osigurati provođenje.

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Izraditi (create) – izraditi politiku privatnosti koja odgovara poslovanju
- Provoditi (maintain) – provoditi politiku privatnosti u svakodnevnom radu
- Uskladiti (uphold) – uskladiti politiku privatnosti s promjenama u organizaciji, tehnologiji, okolini

5.1.8 Dokazivanje

Škola će dokumentirati i biti u mogućnosti pokazati da poštuje principe GDPR te da obrađuje podatke na način koji štiti privatnost ispitanika, posebno za slučaj nadzora AZOP-a (vidi Članak 5.2. GDPR).

Pojedine taktike koje se mogu koristiti su (ali nisu ograničene na):

- Zabilježiti (record) – zabilježiti i dokumentirati na svim nivoima organizacije svaki postupak koji je imao u pozadini obradu osobnih podataka
- Provjeriti (audit) – provesti ispitivanje koje će utvrditi provodi li se utvrđena politika i na koji način te jesu li zadovoljeni svi postavljeni uvjeti i provode li se redovno sve aktivnosti programa privatnosti.
- Izvijestiti (report) – izvijestiti o nalazima provjere nadležne, posebno službenika za zaštitu podataka a on u nekim situacijama i AZOP.

5.2 WB Privacy Program Manager Internet portal

Upravljanje programom zaštite podataka provodi se kroz WB-PPM Internet portal koji je razvijen na online platformi Citrix Podio.

5.2.1 Program privatnosti

Program privatnosti čine sve aktivnosti koje provodi organizacija kako bi provodila utvrđene mjere kao interne kontrole kojima upravlja prepoznatim rizicima.

Elementi programa privatnosti evidentiraju se i dokumentiraju putem aplikacija na portalu Podio (Citrix) pod imenom WB-PPM

5.2.2 Okvir za upravljanje rizicima

„Risk management framework“: pretpostavljeni okvir rizika je GDPR ali može biti i neki drugi poput tehničkih i organizacijskih mjera voditelja obrade ukoliko je organizacija izvršitelj obrade u nekim poslovnim procesima ili standardi poput ISO27000 i ISO27700

Članci: članci GDPR uredbe na koje se referenciraju pojedine aktivnosti programa privatnosti ili drugi dokazi sukladnosti

Recitali: recitali GDPR uredbe

Odjeljci: odjeljci unutar GDPR članka

5.2.3 Obrada zahtjeva ispitanika

Upiti ispitanika evidentiraju se u WB-PPM a mogu se zaprimiti i putem web forme.

5.2.4 Praćenje incidenta i povrede podataka

Svaki incident potrebno je evidentirati u WB-PPM a mogu se primiti i putem web forme.

5.2.5 Okvir programa

PMC: područja rizika (norma, regulativa, standard, TOM i sl.)

PMAF: interne kontrole za pojedina područja rizika, referenciraju se na Članci GDPR

Program: planirane aktivnosti koje će provoditi organizacija za provođenje mjera za jednu ili više internih kontrola, referenciraju se na Članci GDPR

5.2.6 Dokazivanje pouzdanosti

Sukladnost: evidencija provedene jedne ili više aktivnosti iz "Program"

Incident: evidencija i praćenje obrade stvarnog incidenta; incident se može registrirati i putem web linka: <https://podio.com/webforms/25063255/1843957>

SAR: zaprimanje i praćenje obrade upita ili prigovora Ispitanika; zaprimiti se može i putem web linka: <https://podio.com/webforms/25063244/1843956>

Evidencija: evidencija aktivnosti obrada sukladno GDPR Članak 30, ako je primjenjivo

DOKUMENTACIJA - svaki dokument koji može poslužiti kao dokaz prilikom dokazivanja usklađenosti s principima GDPR (pouzdanost) ili drugim kategorijama rizika.

5.2.7 Registar obrada i podataka

OBRADE - katalog obrada osobnih podataka prema GDPR Članku 4.2

OSNOVA - katalog pravnih obaveza obrade osobnih podataka (zakona i sl.) koje se primjenjuju kao zakonitost obrade po GDPR Članku 6.1.c

POHRANA - katalog pohrana (politika čuvanja podataka)

PODATKOVNAKAT - kategorije osobnih podataka

PODACI - pojedinačni podaci prema Članku 4.1 GDPR koji mogu biti direktni ili indirektni identifikatori osoba, ili predstavljaju osjetljive podatke o osobama.

ISPITANICI - kategorije ispitanika prema GDPR Članku 4.1

RIZICI - katalog rizika

PRIVOLE - katalog privola (predložaka) prema GDPR Članku 4.11

5.2.8 Sudionici programa privatnosti

ORGANIZACIJE - sve organizacije koje su na bilo koji način uključene u obradu osobnih podataka kao i treće strane

OSOBE - sve osobe koje čine "privacy network" ili su na bilo koji način uključene u obradu osobnih podataka kao i kontakti Organizacije

5.2.9 Obrada podataka

SUSTAVI - registar svih sustava koji služe obradi osobnih podataka ili su na neki način uključeni u istu, predstavljaju "asset" odn. vrijednost tvrtke koju je potrebno štiti. Mogu biti sustavi za analognu obradu i pohranu podataka (štampani dokumenti i spisi, ormari i sl.) ali i IT sustavi obrade i pohrane kao i telekomunikacijski resursi.

LOKACIJE - sve mikro i makro lokacije na kojima se nalaze predmetni sustavi obrade: soba, ormar, računalo, baza podataka, mrežna mapa i sl.

5.2.10 Prijenos podataka

PRIJENOS - svaki evidentirani prijenos podataka trećim stranama, unutar i van EU

PRIMATELJI - svi primatelji evidentiranih prijenosa podataka

5.2.11 Arhitektura poslovnog sustava

PROCESI - Poslovni procesi, pod-procesi i aktivnosti koji se odvijaju unutar organizacije. Aktivnosti koje se odvijaju u svrhe obrade osobnih podataka odgovaraju GDPR svrhama i obradama osobnih podataka što se nalaze u Evidenciji aktivnosti obrada.

5.3 Pregled obrada koje provodi Škola

5.3.1 Obrade u svrhu provođenja odgojnih i obrazovnih aktivnosti

Vidi WB-PPM

5.3.2 Obrade za podršku rada škole

Vidi WB-PPM

5.4 Klasifikacija osobnih podataka

Škola prilikom obrade osobnih podataka koristi slijedeću klasifikaciju prema ovdje predloženim polaznim kategorijama (u izradi):

5.4.1 Vanjski

- identifikacijski
- fizička karakteristika
- etnički
- ponašanje
- medicinski i zdravstveni
- seksualni
- demografski

5.4.2 Socijalni

- profesionalni
- kriminalni
- komunikacijski
- obiteljski
- društvene mreže

5.4.3 Interni

- znanje i vjerovanje
- preference
- autentikacija

5.4.4 Praćenje

- kontakt
- terminalna oprema
- lokacija

5.4.5 Odgojni

- T.b.d.

5.4.6 Edukativni

- T.b.d.

5.4.7 Financijski

- bankovni račun
- transakcijski podaci
- kreditni podaci
- vlasništvo

5.4.8 Povijesni

- životna povijest

5.4.9 Školski podaci

- T.b.d.