

Smernice za skladno uporabo informacijskih rešitev v šolstvu

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice so namenjene zagotavljanju skladnosti na področju varstva osebnih podatkov pri uporabi IT rešitev v šolstvu.
Ciljne javnosti:	Šole, pooblaščenec osebe za varstvo osebnih podatkov v šolstvu, resorno ministrstvo in drugi odločevalci, ki pripravljajo predpise in politike na področju izobraževanja, ponudniki IT storitev za šole.
Status:	javno
Verzija:	1.0
Datum izdaje:	2. 11. 2021
Avtorji:	Informacijski pooblaščenec, ilustracije: Freepick; Flaticon.
Ključne besede:	Smernice, obdelava osebnih podatkov, pravice posameznika, informiranost posameznikov, evidence dejavnosti obdelave, ocene učinkov na varstvo osebnih podatkov, pogodbeno obdelava, prenos v tretje države, varnost na spletu.



INFORMACIJSKI
POOBLAŠČENEC

KAZALO VSEBINE

1	UVOD	5
2	OSNOVNI POJMI VARSTVA OSEBNIH PODATKOV V PRAKSI	7
2.1	Kaj je osebni podatek?	7
2.2	Kdaj se uporabljajo pravila varstva osebnih podatkov?	7
2.3	Kdo je upravljavec in kdo obdelovalec?	7
3	ZAKONITOST	9
3.1	Namen in pravna podlaga	9
3.2	Najmanjši obseg podatkov	9
3.3	Pravne podlage	10
4	VARNOST IN ODGOVORNOST	14
4.1	Kdaj je obdelava VARNA - zahteve zakonodaje?	14
4.2	Kdaj je obdelava ODGOVORNA - zahteve zakonodaje?	14
5	POGODBENA OBDELAVA IN SKUPNI UPRAVLJAVCI	17
5.1	Kdaj je pogodbena obdelava ustrezno urejena - zahteve zakonodaje?	17
5.2	Skupni upravljavci osebnih podatkov	19
6	PRENOSI V TRETJE DRŽAVE IN MEDNARODNE ORGANIZACIJE	20
6.1	Kdaj gre za prenos?	20
6.2	Pod kakšnimi pogoji je prenos dopusten?	20
7	INFORMIRANJE IN PRAVICE	22
7.1	Informiranje posameznikov (členi 12 -14 Splošne uredbe)	22
7.2	Pravice posameznikov (členi 15 – 22 Splošne uredbe)	25
8	EVIDENCE DEJAVNOSTI OBDELAVE OSEBNIH PODATKOV	29
8.1	Zakaj je treba obdelave osebnih podatkov evidentirati?	29
8.2	Za koga velja obveznost evidentiranja?	29
8.3	Kdaj je evidentiranje obvezno in kdaj ne?	29
8.4	Kaj morajo vsebovati evidence dejavnosti obdelave?	30
8.5	PRIMERI	31
9	OCENA UČINKOV NA VARSTVO OSEBNIH PODATKOV	32
10	KRŠITEV VARNOSTI OSEBNIH PODATKOV	33
10.1	Kaj je kršitev varnosti?	33
10.2	Kako mora ukrepati upravljavec, če zazna kršitev varnosti?	33
10.3	Kakšni sta vloga in odgovornost obdelovalcev?	34

11	VLOGA POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV	35
11.1	Kdo je pooblaščen osebni za varstvo osebnih podatkov?	35
11.2	Kako lahko pomaga pooblaščen osebni za varstvo osebnih podatkov?	36
12	ZAKLJUČEK	37
	Priloga: kontrolni seznam za skladnost	38

1 UVOD

Informacijski pooblaščenec (v nadaljevanju: IP) je v svoji praksi v zadnjem času zaznal večje število vprašanj, ki so se nanašala na izvajanje pouka in drugih šolskih dejavnosti ter organizacijo dela učiteljev z uporabo komunikacijske informacijske tehnologije (v nadaljevanju: IT rešitve). Zlasti v času COVID-19 krize, ko se je uvedel pouk na daljavo, se je pokazala povečana potreba po uporabi teh rešitev. Klasične učilnice so zamenjale videokonference, kjer pride do prenosa slike in glasu učiteljev in učencev po elektronskih omrežjih. Če se je za ta namen uporabljalo najpogostejše spletne storitve, kot npr. Zoom, je lahko prišlo tudi do prenosa osebnih podatkov v tretje države (npr. v ZDA). V praksi so nekateri učitelji zaradi potrebe po izkazovanju opravljenih šolskih nalog (zlasti pri pouku telesne vzgoje), zahtevali posredovanje fotografij ali posnetkov opravljenih dejavnosti. Učitelji so v nekaterih primerih zahtevali tudi, da učenec namesti na pametni telefon in uporablja določeno aplikacijo za beleženje telesne aktivnosti in lokacije – kot dokaz o opravljeni telesni dejavnosti pa pošlje zaslonski posnetek opravljene poti na aplikaciji. Postavilo se je tudi vprašanje digitalne identitete prek uporabe elektronskih naslovov oziroma ustvarjanja uporabniških profilov in elektronskih naslovov za učitelje in učence, ki bi omogočili elektronsko komunikacijo. Vse več se uporabljajo tudi druge IT rešitve, ki omogočajo preverjanje znanja na daljavo, hrambo izdelkov, komunikacijo in podobno (npr. Arnes učilnica).

IT rešitve torej omogočajo raznovrstno komunikacijo učitelj-učenec-starš kot tudi samo organizacijo delovnega procesa s strani delodajalca (uporaba Google storitev za volitve, vodenje evidenc v Google Drive-u itd.). Pri vseh navedenih aktivnostih pride od obdelave osebnih podatkov, zaradi česar je treba zagotoviti pogoje za skladno obdelavo, kot to določa Splošna uredba¹ in drugi predpisi s področja varstva

osebnih podatkov. Vsi procesi, pri katerih pride do obdelave osebnih podatkov z uporabo IT rešitev, so predmet obravnave pričujočih smernic.

Pravila varstva osebnih podatkov po Splošni uredbi vsebujejo mnogo obveznosti preko katerih zagotavljajo posamezniku, da ima določeno mero vpliva nad tem, kdo in zakaj obdeluje njegove osebne podatke. Posameznik mora biti ustrezno informiran o obdelavi (člena 13 in 14 Splošne uredbe), upravljavci morajo posameznikom zagotavljati uresničevanje njihovih pravic (členi 15-22 Splošne uredbe), upravljavec mora zagotavljati ustrezno raven varnosti osebnih podatkov (člen 32 Splošne uredbe), ko je to ustrezno, mora upravljavec izvajati oceno učinkov itd.

Pomemben vidik pri zagotavljanju skladnosti na področju IT rešitev je ustrezna ureditev prenosov osebnih podatkov v tretje države. Zaradi narave delovanja informacijske komunikacijske tehnologije, pri uporabi storitev ponudnikov kot so Google, Microsoft, Zoom itd. (gre za ponudnike, ki imajo svoje strežnike v tretjih državah), pogosto pride do prenosa osebnih podatkov v tretje države. Evropska zakonodaja varstva osebnih podatkov določa posebna pravila za prenos osebnih podatkov zunaj EU – zato, da se zagotovi primerljivo raven varstva osebnih podatkov povsod, kjer se podatki nahajajo. (nekateri države namreč nimajo učinkovitih zakonodajnih in upravno-organizacijskih pogojev za zagotavljanje varstva osebnih podatkov, zato upravljavec, ki je odgovoren za osebne podatke v EU, ne sme pustiti, da se podatki prenašajo nekam, kjer ni zagotovljene primerljive ravni varstva, kot to zahteva evropska zakonodaja). Za zakonit prenos osebnih podatkov v tretje države je na voljo več instrumentov, mora pa jih upravljavec poznati pred pričetkom uporabe IT rešitve.

Upravljavci pogosto tudi zmotno menijo, da če uporabljajo IT rešitev, ki so jo kupili ali brezplačno namestili, da je njena uporaba že zato dopustna. Posebej pogosto je zmotno prepričanje, da je zakonitost obdelave osebnih podatkov zagotovljena že s tem, ko

¹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES (Splošna uredba)

ponudnik izkazuje, da ima za uporabo svoje aplikacije strogo varnostno politiko, ki je morda potrjena z določenimi certifikati (npr. SOC2 tipa 1) ali standardi (npr. ISO). Navedena varnostna zagotovila sicer pomagajo upravljavcu, da lažje izkazuje uporabo IT rešitve skladno s pravili varstva osebnih podatkov, vendar to ni zagotovilo, da je IT rešitev dopustno uporabljati za ta namen (za ponazoritev, uporaba orožja brez orožnega lista in v nasprotju z dovoljenimi nameni je nezakonita ne glede na to, kako varno in certificirano je samo orožje). Za zakonitost obdelave osebnih podatkov pa je v prvi vrsti odgovoren upravljavec osebnih podatkov (šola), ki mora preveriti, ali se zadevna IT rešitev (aplikacija, program, itd.) sme uporabljati za določen namen – torej ali je njena uporaba sploh dopustna. **Upravljavec mora torej zagotoviti, da je obdelava osebnih podatkov, ki jo izvaja z uporabo določene IT rešitve poštena, pregledna in tudi varna.**

Namen pričujočih smernic je tako zagotoviti orodje, s pomočjo katerega bodo lahko šole in učitelji preverili ali izbrana IT rešitev omogoča skladno obdelavo osebnih podatkov IN ali se izbrano IT rešitev uporablja na način, ki je v skladu s pravili varstva osebnih podatkov. Če se ugotovijo pomanjkljivosti, IP pričakuje, da bodo šole ustrezno prilagodile svoja interna pravila ravnanja in za morebitne nejasnosti poiskale odgovore najprej pri svoji pooblaščenici osebni za varstvo osebnih podatkov, v nadaljevanju pa pri pristojnih institucijah (resorno ministrstvo, Zavod za šolstvo, IP). IP upa, da bodo pričujoče smernice v pomoč tudi resornemu ministrstvu pri pripravi potrebnih sistemskih usmeritev in podpore za zagotavljanje skladne obdelave osebnih podatkov v šolstvu pri uporabi IT rešitev.

IP poudarja, da je pri uporabi IT rešitev v šolstvu nujno potreben enoten pristop - idealno na ravni celotne države, najmanj pa na ravni posamezne šole. Odločitev glede uporabe posamezne IT tehnologije ne bi smela biti diskrecija učitelja, saj uporaba tehnologije zaradi narave njenega delovanja prinaša različna tveganja. Ta tveganja zakonodaja naslavlja z ukrepi in pogoji, ki se jih mora zavedati upravljavec osebnih podatkov, ki je po Splošni uredbi tudi odgovoren za skladno ravnanje.

2 OSNOVNI POJMI VARSTVA OSEBNIH PODATKOV V PRAKSI

2.1 Kaj je osebni podatek?

„Osebni podatki“ pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika (člen 4(1) Splošne uredbe).

Izkušnje iz inšpekcijskih nadzorov kažejo, da ponudniki informacijskih storitev pogosto navajajo, da se obdelujejo »zgolj anonimizirani podatki«, v postopku pa se izkaže, da gre za napačno razumevanja koncepta »anonimiziranih podatkov«, saj gre zgolj za »pseudonimizirane podatke«, ki jih je skladno s Splošno uredbo treba obravnavati kot osebne podatke. Takšen primer je dostop ponudnika izbrane IT storitve do podatkov iz zbirke digitalnih identitet, dodeljenih dijakom/študentom, četudi se ti podatki zgolj pseudonimizirano prenesejo ponudniku. Upoštevajoč citirano določbo 4(1) v povezavi z uvodno določbo 26 Splošne uredbe, se načela varstva osebnih podatkov ne uporabljajo zgolj za anonimizirane informacije, ki niso povezane z določenim ali določljivim posameznikom, ali osebne podatke, ki so bili anonimizirani na tak način, da posameznik, na katerega se nanašajo osebni podatki, ni ali ni več določljiv. Anonimizacija osebnih podatkov je alternativa izbrisu, če se upoštevajo vsi ustrezni vsebinski elementi ter se verjetnost in resnost tveganja, vključno s tveganjem ponovne identifikacije redno ocenjujeta.²

2.2 Kdaj se uporabljajo pravila varstva osebnih podatkov?

Pravila varstva osebnih podatkov se uporabljajo, ko se osebni podatki obdelujejo z avtomatiziranimi sredstvi

(npr. prenos podatkov po elektronskih omrežjih) ali ko se podatke obdeluje v elektronsko podprti zbirki osebnih podatkov (npr. vodenje dokumentacije o učencu v sistemu eAsistent ali Lo.Polis). Uporaba IT rešitev, ki prenašajo sliko posameznika, shranjujejo in predvajajo posnetke, prikazujejo profil posameznika, omogočajo ocenjevanje, oblachno hrambo podatkov, merijo telesne aktivnosti itd. so primeri, ko bodisi nastaja zbirka osebnih podatkov (npr. zbirka posnetkov učencev) bodisi se osebni podatki obdelujejo z avtomatiziranimi sredstvi (npr. videokonferenca v živo).

V vseh primerih, ko se uporabljajo pravila varstva osebnih podatkov, je **upravljavec odgovoren**, da zagotovi pogoje za skladno obdelavo posameznih vrst osebnih podatkov, ki jih pridobiva od samih posameznikov ali iz drugih virov – vključno s **pravno podlago za določen in izrecno opredeljen namen, varno obdelavo, informiranjem** posameznikov in uresničevanjem njihovih **pravic** po Splošni uredbi, pogoji za **pogodbeno obdelavo**, pogoji za **prenose v tretje države** (če pri obdelavi pride do tega), **evidentiranjem** dejavnosti obdelave, izvedbo **ocene učinkov na varstvo osebnih podatkov, obveščanjem o kršitvah varnosti**, če pride do varnostnega incidenta ter druge obveznosti po Splošni uredbi.

2.3 Kdo je upravljavec in kdo obdelovalec?

„**Upravljavec**“ po definiciji iz Splošne uredbe pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave. „**Obdelovalec**“ pa pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca.

Ko se prek IT rešitve (npr. Arnes učilnica, videokonferenca) obdelujejo osebni podatki učencev, dijakov in učiteljev, kot upravljavec osebnih podatkov nastopa šola – ta je v odnosu do učencev ali dijakov izobraževalna institucija, v odnosu do učiteljev, profesorjev in drugih zaposlenih pa delodajalec. Ker je upravljavec osebnih podatkov šola, se šteje, da učitelji delujejo v imenu šole in po navodilih svojih nadrejenih. **Slednje velja praviloma tudi v primeru, ko učitelj brez**

² Stališče Delovne skupine po členu 29 iz »Mnenja 05/2014 o anonimizacijskih tehnikah«, WP 216, 10. april 2014.

navodil nadrejenega namesti, uporablja in zahteva od učencev uporabo določene IT rešitve pri izvajanju pouka. Redko je namreč mogoče utemeljiti, da je učitelj deloval izključno v lastnem imenu in tako samovoljno zahteval od svojih učencev uporabo določene IT rešitve v nasprotju z internimi pravili šole (ali zaradi odsotnosti internih pravil) in tako deloval kot upravljavec osebnih podatkov. Kadar se IT rešitev uporablja za izvajanje izobraževalne dejavnosti, pa tudi ni mogoče trditi, da je učitelj ravnal v okviru svoje popolnoma osebne ali domače dejavnosti (za izvajanje popolnoma osebne ali domače dejavnosti se Splošna uredba ne uporablja)³.



Pri uporabi informacijske storitve, ki omogoča elektronsko komunikacijo (npr. videokonferenca), vedno pride do posredovanja osebnih podatkov preko strežnika, ki ga običajno zagotavlja ponudnik te informacijske storitve. Ker mora ponudnik (npr. Arnes) za zagotavljanje svoje storitve shraniti in posredovati naprej podatke od sporočevalca do naslovnika, pri tem nujno pride do obdelave osebnih podatkov, ki jo izvede ponudnik informacijske storitve. Pravila varstva osebnih podatkov pa zahtevajo, da se obdelava izvaja pod vodstvom in po dokumentiranih navodilih upravljavca ter da ima upravljavec nadzor tudi nad tem, kdo in pod kakšnimi pogoji podatke v njegovem imenu obdela. Zato mora upravljavec s ponudnikom, ki zanj obdeluje osebne podatke (npr. Arnes), skleniti pisno pogodbo o obdelavi osebnih podatkov, v kateri se zapiše pogoje obdelave (npr. kakšno varnost bo ponudnik zagotavljal;

kje bo podatke hranil; komu jih bo posredoval ipd.). Bistvene sestavine pogodbe o obdelavi osebnih podatkov (torej kaj vse mora vsebovati pogodba o obdelavi) natančno določa člen 28(2) Splošne uredbe. Ponudnik informacijske storitve v tem primeru nastopa v vlogi **obdelovalca osebnih podatkov**, ki sme delovati samo v imenu upravljavca in le po njegovih navodilih, ki so zapisana v obvezni pisni pogodbi o obdelavi osebnih podatkov.

Realnost aktualne informacijske družbe pa je takšna, da imajo upravljavci (npr. šole) lahko le majhen vpliv na to, pod kakšnimi pogoji bo tehnološki velikan (npr. Zoom, Microsoft, Google) ponudil svojo storitev – npr. koliko bo pripravljen prilagajati pogoje pogodbene obdelave, da bodo ti skladni z evropsko in slovensko zakonodajo o varstvu osebnih podatkov. Za izbiro ponudnika pa je kljub vsemu odgovoren upravljavec – to je šola. Če šola uporablja spletne storitve svetovnih tehnoloških podjetij, se mora zavedati, da s tem nase prevzema tveganja za neskladne pogodbe, neskladne pogoje za prenose v tretje države ipd. Četudi se nadzorni organi in države EU trudijo tudi z velikimi spletnimi ponudniki storitev zagotoviti spoštovanje zakonodaje, je skladnost na tem nivoju težko doseči, odgovornost v konkretnem primeru pa je na upravljavcu osebnih podatkov, torej na šoli. **Zato je nadvse pomembno, da se šole skupaj z Ministrstvom za šolstvo, Zavodom za šolstvo in šport RS ter drugimi deležniki trudijo vzpostaviti enotno prakso pri določitvi meril za izbiro ponudnikov, ki ponujajo IT rešitve šolam – da bodo lahko šole izbrale takšne ponudnike, ki zagotavljajo po eni strani učinkovito izvajanje izobraževalnega dela po drugi strani pa zagotavljajo skladnost s predpisi s področja varstva osebnih podatkov.**

³ 2(1)(c) Splošne uredbe določa, da se ta uredba ne uporablja za obdelavo osebnih podatkov s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti.

3 ZAKONITOST

3.1 Namen in pravna podlaga

Vsakočas ko šola obdeluje osebne podatke (npr. zbira, pridobiva ali posodablja kontaktne podatke, zahteva posredovanje posnetkov/fotografij učencev, izvaja ocenjevanje, objavlja podatke) se mora zavedati, kaj želi s konkretno obdelavo doseči – to je **namen obdelave**, ki mora biti **določen, izrecen in zakonit**.

Nameni, za katere šola obdeluje osebne podatke, so lahko različni, npr: *izvajanje izobraževalnih dejavnosti, komunikacija s starši, organizacija dela šole, promocijske aktivnosti, objave zaradi obveščanja javnosti, spodbujanje (prostovoljnega) udejstvovanja učencev* itd. Opredelitev namena je bistvenega pomena za zakonito obdelavo osebnih podatkov, saj je z namenom neposredno povezana **pravna podlaga za obdelavo osebnih podatkov**.

Primer: Osnovna šola na podlagi Zakona o osnovni šoli (95. člen) vodi zbirko podatkov o učencih, vpisanih v osnovno šolo, in njihovih starših, ki obsega: (1) podatke o učencih: ime in priimek ter EMŠO, spol, datum, kraj in država rojstva, prebivališče in državljanstvo, zdravstvene posebnosti, katerih poznavanje je nujno za učenčevo varnost in za delo z učencem in (2) podatke o starših: ime, priimek, naslov prebivališča, telefonska številka, na katero je mogoče posredovati nujna sporočila v času, ko je učenec v šoli. Gre za zbirko, ki se vodi za namen obveznega izobraževanja in je izrecno zakonsko predpisana. Podlaga za zbiranje in obdelavo osebnih podatkov za ta namen izvira neposredno iz zakona.

Primer: Učitelj pri izvajanju pouka na daljavo uporablja videokonferenčni sistem, ki omogoča prenos žive slike. Pri tem pride do avtomatizirane obdelave osebnih podatkov. Gre za obdelavo, ki se izvede v zvezi z izobraževanjem, kar je javnopravna obveznost

šole in je regulirana s predpisi. Podlaga za zbiranje in obdelavo osebnih podatkov za ta namen izvira iz potrebe po izvajanju javnopravne naloge šole oziroma njene zakonite pristojnosti.

Primer: Šola objavi fotografije z imeni in priimki najboljših iz šolskega športnega tekmovanja na svoji spletni strani. Namen je promocija dogajanja na šoli kar nima zveze z izobraževanjem. Objava na spletni strani za namen promocije šole ni regulirana s predpisi. Podlaga za obdelavo za namen promocije je lahko privolitev učenca oziroma privolitev staršev ali skrbnikov.

3.2 Najmanjši obseg podatkov

Za zakonito obdelavo je zlasti pomembno tudi načelo **najmanjšega obsega podatkov**. To načelo zahteva, da so osebni podatki **ustrezni, relevantni in omejeni na to, kar je potrebno** za namene, za katere se obdelujejo.

Če zakon izrecno predpisuje, katere podatke je dopustno zbirati in hraniti (npr. zbirka podatkov o učencih, vpisanih v osnovno šolo, in njihovih starših po 95. členu Zakona o osnovni šoli)⁴ potem je načelo najmanjšega obsega podatkov opredelil že zakonodajalec in upravljavec (šola) ne sme zbirati drugih podatkov kot določa zakon za zakonsko opredeljen namen. Če pa zakon izrecno ne predpiše podatkov in zbirke, vendar je obdelava *nujno potrebna* za izvajanje javnopravne naloge ali pristojnosti šole, ki izvira iz zakona, potem mora upravljavec sam presoditi, ali je v skladu z načelom najmanjšega obsega podatkov, da podatke v konkretnem primeru obdeluje pod pogoji iz četrtega odstavka 9. člena ZVOP-1 (več o tem v pod poglavju 3.3.2).

Primer: Učitelj športne vzgoje zahteva od učencev, ki se šolajo na daljavo, da pretečejo tri kilometre. Da bi lahko spremljal njihovo aktivnost, zahteva, da namestijo na pametni telefon aplikacijo, ki beleži njihovo gibanje in

⁴ Drugi odstavek 95. člena Zakona o osnovni šoli (Uradni list RS, št. 81/06 – uradno prečiščeno besedilo, 102/07, 107/10, 87/11, 40/12 – ZUJF, 63/13 in 46/16 – ZOFVI-L)

lokacijo, kot dokaz o izvedeni aktivnosti pa posredujejo zaslonsko sliko opravljene poti iz aplikacije. Kot izhaja iz mnenja [IP št. 07121-1/2020/2025, z dne 11. 11. 2020](#)⁵, »takšne aplikacije in pametne naprave zbirajo in obdelujejo vrsto, lahko tudi občutljivih osebnih podatkov, in sicer praviloma na podlagi privolitve, ki pa pri izobraževanju na daljavo kot javnopravni nalogi ni ustrezna pravna podlaga. Uporaba tovrstnih aplikacij oziroma pametnih naprav za preverjanje izpolnjevanja nalog tudi ni izrecno zakonsko predpisana.« Zahteva učitelja, da se naloži aplikacija, tako ni v skladu z načelom najmanjšega obsega podatkov, saj učitelj s svojo avtoriteto zahteva, da se učenci kot uporabniki aplikacije, podvržejo režimu obdelave podatkov, ki ga predvideva ponudnik aplikacije za prostovoljne uporabnike. To pa je občutno nesorazmerno za namen izkazovanja naloge pri telesni vzgoji, ki je javnopravna naloga šole.

3.3 Pravne podlage

3.3.1 Splošno

Splošna uredba določa, katere so lahko dopustne pravne podlage za obdelavo osebnih podatkov – v javnem ali zasebnem sektorju. Po členu 6(1) je obdelava zakonita, če se ta vrši na eni od naslednjih podlag:

- (a) **privolitev** posameznika⁶,
- (b) izvajanje **pogodbe s posameznikom**, aktivnosti pred sklenitvijo pogodbe,
- (c) izvajanje **zakonske** obveznosti,
- (d) zaščita življenjskih interesov,
- (e) izvajanje **javne oblasti** ali **naloge v javnem interesu** (v javnem sektorju),
- (f) **zakoniti interesi** (v zasebnem sektorju).

Strožji režim (strožji splošni pogoji) velja za t.i. **posebne vrste osebnih** podatkov, ki so bolj občutljive narave. To so podatki, ki zajemajo raso ali etnično poreklo; politično mnenje; versko ali filozofsko prepričanje;

članstvo v sindikatu; obdelava genetskih podatkov; biometričnih podatkov za namene edinstvene identifikacije posameznika; podatki v zvezi z zdravjem; podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo. Njihova obdelava je načeloma prepovedana, dopustna pa le pod strogimi pogoji, ki jih določa **člen 9(2)** Splošne uredbe.

3.3.2 Pravne podlage v javnem sektorju

Šola kot izvajalec javne službe (in v določenem delu tudi izvajalec javnih pooblastil) osebne podatke za namene izvajanja svojih zakonskih pristojnosti (za potrebe (obveznega) izobraževanja), obdeluje na način, ki velja za obdelave osebnih podatkov v javnem sektorju. V poštev prideta zlasti določbi 6(1)(c) in 6(1)(e) Splošne uredbe. Ob tem velja dodati, da skladno z določbama 6(2) in 6(3) Splošne uredbe, se v javnem sektorju – kamor sodijo tudi šole, uporablja nacionalna ureditev. Zato je treba upoštevati tudi 9. člen Zakona o varstvu osebnih podatkov (v nadaljevanju: ZVOP-1),⁷ ki splošno ureja pravne podlage za obdelavo osebnih podatkov v javnem sektorju. 9. člen ZVOP-1 kot pravilo določa, da se smejo osebni podatki obdelovati le, če osebne podatke in obdelavo osebnih podatkov določa zakon (prvi odstavek 9. člena ZVOP-1) – primer je prej navedeni 95. člen ZOsn, ki določa katere podatke šola sme voditi in obdelovati za namen obveznega izobraževanja. Če ne gre za oblastno delovanje šole, lahko šola osebne podatke obdeluje na podlagi veljavne privolitve (smiselno drugi odstavek 9. člena ZVOP-1). Izjemoma se lahko v javnem sektorju obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo (četrti odstavek 9. člena ZVOP-1).

Treba je poudariti, da po slovenski Ustavi (38. člen) obdelavo osebnih podatkov lahko določi le zakon. Četrti odstavek 9. člena ZVOP-1 sicer tudi zagotavlja neposredno zakonsko podlago za obdelavo osebnih

⁵ <https://www.ip-rs.si/mnenja-gdpr/6048a6413419b>.

⁶ Več informacij: [spletna stran IP o privolitvi](#).

⁷ Uradni list RS, št. 94/07-UPB1 in 177/20

podatkov, vendar pa je lahko takšna obdelava le IZJEMOMA dopustna, če je

- (1) NUJNA za izvajanje zakonsko predpisane pristojnosti šole in
- (2) ne sme posegati v UPRAVIČEN INTERES POSAMEZNIKA.

Ker gre za izjemo od splošnega pravila, da lahko obdelavo osebnih podatkov določi le zakon, je treba to podlago presojski strogo. Zato tudi IP v inšpekcijskih postopkih izpolnjenost pogojev po četrtem odstavku presoja strogo. Za izkaz NUJNOSTI obdelave mora upravljavec izkazati, da je bila to edina možnost glede na dane okoliščine, da sploh lahko izvaja svojo zakonito pristojnost, nalogo ali obveznost (npr. zaradi karantene pouk ni mogel potekati drugače, kot z uporabo videokonferenčnih sistemov, zato je obdelava osebnih podatkov, ki se pri tem izvede, *nujna*).

Drugi pogoj je, da obdelava *ne sme posegati v upravičen interes posameznika*. V tem pogoju se zrcali standard *upravičenega pričakovanja zasebnosti*, ki ga je razvilo Evropsko sodišče za človekove pravice (ESČP), ki v bistvu kaže na uporabo načela sorazmernosti v ožjem smislu (torej tehtanje med ciljem, ki je v javnem interesu in ga obdelava izpolnjuje proti interesu posameznika, da se v njegove pravice ne posega). Za uravnoteženje tega cilja so ključne tudi morebitne dodatne varovalke, ki preprečujejo neupravičeno obdelavo osebnih podatkov (npr. pošteno in ustrezno obveščanje posameznikov, obzirnost pri zahtevah glede obvezne »vključenosti kamere« ali drugi organizacijski ukrepi, dodatni varnostni ukrepi, kot je šifriranje in kriptiranje podatkov med prenosom itd).

Vse navedeno lahko prispeva k dopustnosti obdelave v konkretnem primeru na podlagi četrtega odstavka 9. člena ZVOP-1, ki pa je, kot omenjeno, zgolj izjemoma dopustna.

Ob zgoraj navedenem je treba dodati, da kadarkoli obdelava osebnih podatkov ni neposredna zakonska obveznost upravljavca, bo podlaga za obdelavo osebnih

podatkov v javnem sektorju izhodiščno izvirala iz določbe 6(1)(e) Splošne uredbe. To pomeni, da ima posameznik v tem primeru pravico, da ugovarja obdelavi osebnih podatkov v skladu s členom 21 Splošne uredbe.

Navedena pravila določajo splošni okvir za razlago konkretne obdelave osebnih podatkov. Ko gre za izvrševanje nalog in pristojnosti javnega sektorja je treba upoštevati področno zakonodajo – tako v primeru, ko osebne podatke in namene obdelave neposredno določa zakon (prvi odstavek 9. člena ZVOP-1), kot tudi, ko podlaga izvira iz pristojnosti, naloge ali obveznosti javnega sektorja pod pogoji iz četrtega odstavka 9. člena ZVOP-1.

3.3.3 Področna zakonodaja, ki ureja pristojnosti šol za izvajanje njihovih javnopravnih nalog

Zakonsko obveznost v zvezi z izvajanjem vzgoje in izobraževanja široko opredeljujejo zakoni s področja osnovnošolskega in srednješolskega izobraževanja, med drugim Zakon o osnovni šoli (v nadaljevanju: ZOsn)⁸, Zakon o gimnazijah (v nadaljevanju: ZGim)⁹ ter Zakon o poklicnem in strokovnem izobraževanju (v nadaljevanju: ZPSI-1),¹⁰ ki določajo obveznost šol, da zagotavljajo predvidene oblike izobraževanja, ter dolžnost učencev in dijakov, da izpolnjujejo svoje šolske obveznosti. Delovne obveznosti učiteljev so opredeljene tudi v Zakonu o organizaciji in financiranju vzgoje in izobraževanja (v nadaljevanju: ZOFVI)¹¹, ki v 119. členu določa tudi "zbiranje in obdelavo podatkov v zvezi z opravljanjem vzgojno-izobraževalnega in drugega dela". **V okviru teh zakonov pa je po mnenju IP treba razlagati tudi vsakršno obdelavo osebnih**

⁸ Uradni list RS, št. 81/06 – uradno prečiščeno besedilo, 102/07, 107/10, 87/11, 40/12 – ZUJF, 63/13 in 46/16 – ZOFVI-K

⁹ Uradni list RS, št. 1/07 – uradno prečiščeno besedilo, 68/17, 6/18 – ZIO-1 in 46/19

¹⁰ Uradni list RS, št. 79/06, 68/17 in 46/19

¹¹ Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 36/08, 58/09, 64/09 – popr., 65/09 – popr., 20/11, 40/12 – ZUJF, 57/12 – ZPCP-2D, 47/15, 46/16, 49/16 – popr., 25/17 – ZVaj in 123/21

podatkov, ki se izvajajo za namen izvajanja vzgoje in izobraževanja, kot javnopravne naloge oziroma javne službe – upošteva zgoraj navedene kriterije, ki izvirajo zlasti iz 9. člena ZVOP-1.

IP je v več svojih mnenjih že poudaril, da bi zaradi izjemnih okoliščin zaradi uveljavljenih ukrepov za preprečevanje širjenja virusa COVID-19, ki so začasno spremenili tudi izobraževalni proces, Ministrstvo za izobraževanje, znanost in šport moralo obstoječo pravno podlago ustrezno pojasniti z enotnimi navodili šolam. Takšen pristop narekuje tudi Splošna uredba v drugem pododstavku člena 6(3), ki določa da se »namen obdelave določi v navedeni pravni podlagi ali pa je v primeru obdelave iz točke (e) odstavka 1 potreben za opravljanje naloge, ki se izvajajo v javnem interesu, ali pri izvajanju javne oblasti, dodeljene upravljavcu. Navedena pravna podlaga lahko vključuje posebne določbe, s katerimi se prilagodi uporaba pravil iz te uredbe, med drugim: splošne pogoje, ki urejajo zakonitost obdelave podatkov s strani upravljavca; vrste podatkov, ki se obdelujejo; zadevne posameznike, na katere se nanašajo osebni podatki; subjekte, katerim se osebni podatki lahko razkrijejo, in namene, za katere se lahko razkrijejo; omejitve namena; obdobja hrambe; ter dejanja obdelave in postopke obdelave, vključno z ukrepi za zagotovitev zakonite in poštene obdelave, kot tiste za druge posebne primere obdelave iz poglavja IX. Pravo Unije ali pravo države članice izpolnjuje cilj javnega interesa in je sorazmerno z zakonitim ciljem, za katerega si prizadeva.«

Pri uporabi IT rešitev pa pride tudi do obdelave osebnih podatkov učiteljev (npr. prenos slike in glasu po elektronskem omrežju). Ko učitelji izvajajo pouk z uporabo IT rešitev, delujejo v vlogi zaposlenih, upravljavec njihovih osebnih podatkov pa je delodajalec (šola). Zunanji izvajalci, ki zagotavljajo delovanje sistema (npr. Arnes, Zoom) pa v razmerju do šole nastopajo kot obdelovalci. **Pravno podlago za obdelavo osebnih podatkov učiteljev mora imeti upravljavec –**

torej šola. Ko šola torej obdeluje osebne podatke svojih zaposlenih, mora ravnati v skladu s področno delovno-pravno zakonodajo. Položaj učiteljev je z vidika razmerja podrejenosti podoben položaju učencev, pri čemer je treba zakonitost obdelave njihovih osebnih podatkov razumeti zlasti v okviru izvrševanja njihovih pravic in obveznosti iz delovnega razmerja. Delovno razmerje učiteljev krovno ureja Zakon o delovnih razmerjih,¹² za javne uslužbenke pa velja tudi Zakon o javnih uslužbencih.¹³ Konkretnjša pravila pa izhajajo iz kolektivnih pogodb in pogodb o zaposlitvah.

Več o obdelavi osebnih podatkov v delovnih razmerjih vsebujejo smernice IP:

➔ [Varstvo osebnih podatkov v delovnih razmerjih](#).¹⁴

3.3.4 Privolitev

V določenih primerih lahko kot pravna podlaga za obdelavo osebnih podatkov pride v poštev tudi **privolitev**. Vendar, če privolitev ni prostovoljna, konkretna, informirana in nedvoumna, ne more biti veljavna. Pri ugotavljanju, ali je bila privolitev dana prostovoljno, se med drugim zlasti upošteva, ali je izvajanje pogodbe, vključno z zagotavljanjem storitve (tudi storitvenih obveznosti javnega sektorja), pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe. Za obdelavo osebnih podatkov učencev, ki so že po naravi razmerja v podrejenem položaju, prostovoljnosti načeloma ni mogoče utemeljiti. Zato je obdelava osebnih podatkov na podlagi privolitve praviloma dopustna le izjemoma, če tako **izrecno predvideva zakon** (npr. podatke o gibalnih sposobnostih in morfoloških značilnostih učencev po 95. členu ZOsn) in **ko ne gre za izvajanje zakonskih pristojnosti** (npr. ko ne gre za izvajanje pouka, temveč na primer promocijo šole in zato morebitna zavrnitev privolitve nima vpliva na izobraževalni proces za učenca).

¹² Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19 in 203/20 – ZIUPOPĐVE

¹³ Uradni list RS, št. 63/07 – uradno prečiščeno besedilo, 65/08, 69/08 – ZTFI-A, 69/08 – ZZavar-E, 40/12 – ZUJF, 158/20 – ZIntPK-C in 203/20 – ZIUPOPĐVE

¹⁴ <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/varstvo-osebni-podatkov-v-delovnih-razmerjih>

Podobno velja tudi za osebne podatke učiteljev, ki so v delovnem razmerju do upravljavca – šole. Privolitev v delovnem razmerju praviloma ni veljavna, ker se zaradi neenakovrednega razmerja (delavec – delodajalec) šteje za prisiljeno. Čeprav se lahko navidez zdi, da je uporaba IT rešitev pri pouku stvar avtoritarne odločitve učitelja, temu praviloma ni tako, saj je šola (upravljavec) odgovorna za skladno uporabo IT rešitev s katero se obdeluje osebne podatke učiteljev – tudi ko ti izvajajo pouk, saj pri tem opravljajo svoje delo za delodajalca. Po stališču IP je privolitev v delovnih razmerjih dopustna le izjemoma, ko delodajalec izkaže, da bi zaposleni lahko zavrnil (in tudi kasneje kadarkoli preklical) privolitev za obdelavo svojih osebnih podatkov, brez škodljivih posledic za njegovo delovno razmerje.

Po stališču IP iz mnenja št. 07121-1/2020/2025, nikakor ni dopustno zahtevati obveznega nameščanja aplikacij, ki beležijo vadbo na pametnem telefonu in ob tem pridobivati podatke o lokaciji ter druge podatke uporabnika na zasebne mobilne telefone učencev.

Pojasniti je treba tudi, da so lahko po 157. členu **Zakona o elektronskih komunikacijah** (v nadaljevanju: ZEKom-1),¹⁵ tehnologije za pridobivanje podatkov s terminalne opreme uporabnikov uporabljene le, če posameznik v to privoli oziroma v primerih nujnih izjem, če je to potrebno zaradi zagotavljanja storitve. **V ta okvir sodijo tudi aplikacije, ki si jih posamezniki namestijo na pametni telefon. Kakršna koli raba tovrstnih aplikacij je lahko le prostovoljna.** Navedeno pa velja tudi, ko šola od učiteljev (zaposlenih) ali učencev/dijakov zahteva namestitve aplikacije na zasebno napravo, pri čemer že sama aplikacija zbira osebne podatke (to so večinoma

vse na spletu dostopne aplikacije, ki beležijo telesno aktivnost, omogočajo konferenčne klice ipd.).

Več o privolitvi:

- ➔ [Pojasnilo o privolitvi na spletni strani IP](#)¹⁶
- ➔ [Smernice 05/2020 o soglasju v skladu z Uredbo 2016/679](#)¹⁷



¹⁵ Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17

¹⁶ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/kliju%C4%8Dna-podro%C4%8Dja-uredbe/privolitev>

¹⁷ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_sl

4 VARNOST IN ODGOVORNOST

→ [Smernice IP o zavarovanju osebnih podatkov](#)¹⁹

4.1 Kdaj je obdelava VARNA - zahteve zakonodaje?

Upravljalavec je dolžan skrbeti za varnost osebnih podatkov v vseh fazah obdelave. Člen 32(1) Splošne uredbe določa, da morata upravljalavec in obdelovalec ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotoviti ustrezno raven varnosti glede na tveganje. **Zagotavljanje varnosti osebnih podatkov je lahko posebej problematično pri uporabi spletnih IT rešitev, ki jih učitelji uporabljajo po lastni presoji in po možnosti brez vnaprejšnjega preudarka o informacijski varnosti.** IP zato ponovno poudarja, da mora šola kot upravljalavec pred pričetkom uporabe posamezne IT rešitve ustrezno ovrednotiti z vidika zagotavljanja varnosti in - če je le mogoče - do izbire teh IT rešitev pristopiti poenoteno.

Večina najbolj uveljavljenih IT rešitev za spletno komuniciranje omogoča t.i. šifriranje od vira do ponora komunikacije (angl. »*end-to-end encryption*«), ne pa nujno v vseh primerih (to najverjetneje npr. ne bo zagotovljeno, če je klic (deloma) opravljen preko navadne telefonske linije in ne preko podatkovnega prenosa) in ne nujno kot privzeto nastavitvev. Razlike med IT rešitvami pa obstajajo tudi glede drugih vidikov varnosti in zasebnosti. **Zato je v svojih mnenjih in pozivih IP priporočil, da se glede vidikov varne obdelave osebnih podatkov pred uporabo upravljalavec osebnih podatkov (ali celo ministrstvo pri pripravi ustreznih priporočil) posvetuje s svojimi pooblaščenimi osebami za varstvo osebnih podatkov in strokovnjaki na področju informacijskih tehnologij.**

Več o varnosti (zavarovanju) osebnih podatkov:

→ Spletna stran IP: [Zavarovanje oz. varnost osebnih podatkov](#)¹⁸

4.2 Kdaj je obdelava ODGOVORNA - zahteve zakonodaje?

Za zakonitost obdelave osebnih podatkov so odgovorne šole in njihova dolžnost je, da so pri izkazovanju zakonitosti tudi proaktivne. V skladu s členom 24 Splošne uredbe so torej šole dolžne sprejeti »ustrezne ukrepe« in »politike«, kar konkretno pomeni, da posamezna šola sprejme podrobnejša interna pravila z navodili za ravnanje in pogoji za skladno obdelavo osebnih podatkov pri izvajanju svojih dejavnosti. Pri tem se šole ne morejo sklicevati na odgovornost ministrstva, zavoda in drugih deležnikov, četudi bi navedeni lahko pomagali šolam pri izpolnjevanju njihovih dolžnosti. Kljub temu pa je treba ponovno poudariti, da je za skladno delovanje na področju varstva osebnih podatkov odgovoren upravljalavec – to je šola. IP pa ob navedenem spodbuja tudi resorno ministrstvo, Zavod za šolstvo in druge deležnike, da pomagajo šolam z enotnimi usmeritvami, kako lahko zagotovijo skladnost na področju varstva osebnih podatkov.

Načelo odgovornosti (*t.i. accountability principle*) iz Splošne uredbe zahteva od upravljalca osebnih podatkov, da **zagotavlja skladnost s pravili** varstva osebnih podatkov ter **da je skladnost sposoben izkazati**. V členu 24 Splošna uredba določa, da ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljalavec izvede ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s to uredbo. Ti ukrepi se pregledajo in dopolnijo, kjer je to potrebno. V drugem odstavku člena 24 Splošna uredba določa, da

¹⁸ <https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljalavcev/zavarovanje-oz-varnost-osebnih-podatkov>

¹⁹ https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf

kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi iz odstavka 1 vključujejo izvajanje ustreznih politik za varstvo podatkov s strani upravljavca.

Glede na navedeno bi bilo ustrezno, da šole oblikujejo ustrezna navodila:

- **katere IT rešitve** naj se uporabljajo za posamezen namen uporabe;
- **kako morajo uporabniki** (učitelji, učenci) **prilagoditi pogoje uporabe** (npr. nastavitve zasebnosti, nastavitve šifriranja med prenosom, itd.) posamezne informacijske rešitve, da bo zagotovljena zahtevana raven varnosti osebnih podatkov.

Prav navedeno – izbira ponudnika IT rešitve in nastavitve pogojev uporabe te rešitve – je tudi predmet zahtev iz člena 25 Splošne uredbe, ki ureja »*vgrajeno in privzeto varstvo osebnih podatkov*«. Zahteva iz člena 25 narekuje, da upravljavec zagotovi **učinkovite mehanizme** za varstvo osebnih podatkov posameznikov. To vključuje, da mora upravljavec **upravljati (obvladovati) in imeti nadzor nad vsemi sredstvi, s katerimi obdeluje osebne podatke** (aplikacije, spletni obrazci, računalniški programi, organizacijski postopki, itd.) **v vseh fazah obdelave osebnih podatkov – tudi ko obdelavo izvaja pogodbeni obdelovalec**. Ko upravljavec obdelavo izvaja sam, mora sprejeti ustrezna interna pravila in preverjati ali se ta pravila spoštujejo. Ko upravljavec obdelavo zaupa pogodbenemu obdelovalcu, je upravljavec **odgovoren za izbiro** ustreznega obdelovalca, za **sklenitev ustrezne pogodbe** o obdelavi osebnih podatkov (s katero obdelovalca zaveže, da ravnava po njegovih dokumentiranih navodilih) in **za nadzor nad izvajanjem** te pogodbe. Vse navedeno upravljavec mora izvajati tako, da sledi temeljnemu načelom varstva osebnih podatkov.

Nadzor nad celotnim procesom obdelave osebnih podatkov (zlasti tistih, ki jih izvaja sam), mora upravljavec izvajati nenehno, torej tudi po vpeljavi novih rešitev, saj mora za zagotavljanje spoštovanja temeljnih načel slediti tudi tehničnemu napredku in posodabljati tehnologijo v skladu z najnovejšim

tehnološkim napredkom. Navedeno sicer ne pomeni, da mora upravljavec slediti »trendom« in si zagotoviti vse najnovejše aplikacije ali programe, ki zagotavljajo najbolj vrhunsko uporabniško izkušnjo. Pomeni pa, da mora upravljavec slediti razvoju tehnologije na trgu, ki izpolnjuje cilje obdelave osebnih podatkov, ki jih zasleduje upravljavec in izbrati tisto rešitev, ki najbolj sledi načelom varstva osebnih podatkov.

Treba je poudariti, da je za obdelavo v prvi vrsti odgovoren **upravljavec**. Obdelovalec je odgovoren kot samostojni upravljavec le, če deluje izven dokumentiranih navodil upravljavca. Zato je glede odgovornosti zelo pomembno, kaj določa pogodba o obdelavi osebnih podatkov. Ni pa odgovoren razvijalec programske opreme ali druge tehnične rešitve za skladno obdelavo osebnih podatkov z uporabo »njegove« IT rešitve. V uvodni določbi 78 Splošna uredba določa, da »**bi bilo treba proizvajalce produktov, storitev in aplikacij spodbujati, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja, zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov**«. **Z drugimi besedami, upravljavec (šola), ki uporablja pripravljene tehnološke rešitve za obdelavo osebnih podatkov (npr. Zoom, Dropbox itd.), se mora pred njihovo uporabo prepričati, da rešitev »vgrajeno« zagotavlja ustrezno varstvo osebnih podatkov.**

***Primer:** Šola se odloča o uporabi nove IT rešitve. Ugotavlja, da nekateri ponudniki ponujajo svoje storitve z uporabo različnih spletnih vtičnikov, ki v pogojih uporabe predvidevajo tudi dostop s strani »pogodbenih partnerjev iz tretjih držav«. Šola mora preveriti, ali so zagotovljeni vsi pogoji za skladno obdelavo osebnih podatkov – zlasti tudi, ali se bodo podatki uporabljali zgolj za namen zbiranja ali morebiti pogodba o obdelavi predvideva uporabo, ki presega namen za katerega ima šola pravno podlago (npr. hrambo podatkov učencev za namen izobraževanja). V primeru sprejema takšnih pogojev bi bila lahko šola odgovorna, ker dovoljuje uporabo pogodbenemu obdelovalcu za (sicer lahko tudi*

»izsiljen«) namen, za katerega sama nima pravne podlage. Ob tem velja pojasniti, da za pogodbe o obdelavi ne veljajo zahteve po jasnosti in razumljivosti, kot to velja za informiranje posameznikov po členu 12 Splošne uredbe. Šola v pogodbeni razmerja vstopa v vlogi pravne osebe, za katero se predvideva višja stopnja skrbnosti, kot pa za posameznike, ki vstopajo v pravna razmerja v svojem imenu.

Z vidika načela pregledne obdelave osebnih podatkov mora upravljavec (šola) »vgrajeno« zagotoviti tudi, da se tudi pri uporabi aplikacij in informacijskih rešitev posameznikom posreduje ustrezne informacije po členu 13 in/ali 14 Splošne uredbe. V praksi so pogosti primeri, ko se posameznike glede informacij v zvezi z obdelavo osebnih podatkov naslavlja na politike zasebnosti pri obdelovalcu, ki zagotavlja storitev, ki pa so pogosto v angleškem jeziku. Z vidika preglednosti obdelave osebnih podatkov takšno sklicevanje ni ustrezno, saj bi skladno s členom 12 Splošne uredbe posamezniki morali dobiti **informacije v enostavno dostopni in razumljivi obliki ob upoštevanju posebnih okoliščin tipičnega posameznika, ki so mu informacije namenjene.**

»Privzeto« varstvo osebnih podatkov pa vzpostavlja obveznost za upravljavca, da sredstva s katerimi obdeluje osebne podatke (programi, aplikacije, procesi), prilagodi tako, da se obdelava osebnih podatkov izvaja v najmanjšem možnem obsegu. Upravljavec mora tako zlasti paziti, da se:

- obdeluje minimalna količina podatkov;
- izvaja minimalni obseg obdelav;
- zagotavlja minimalni čas hrambe;
- podeli minimalno dostopnih pravic.

Upravljavec je torej odgovoren, da zagotovi obdelavo osebnih podatkov, ki bo skladna s Splošno uredbo, tudi če samo sredstvo (npr. aplikacija, sistemska rešitev, itd.) omogoča funkcionalnosti, ki presegajo dopustno mero obdelav osebnih podatkov. Upravljavec torej mora »nastaviti« sredstva tako, da bo pri njihovi uporabi za obdelavo osebnih podatkov sledil načelom Splošne uredbe, zlasti načeloma najmanjšega obsega podatkov in omejitve namena.

Primer: Učitelj pri pisnem ocenjevanju znanja prek videokonference, da bi zmanjšal možnost prepisovanja, zahteva, da imajo učenci vklopljenih več kamer hkrati, ki snemajo celoten prostor, kjer učenec izpolnjuje test. Zaradi prostorske stiske, so v istem prostoru z učencem tudi drugi domači, ki jih učitelj ravno tako vidi na kameri. Po mnenju IP ni v skladu z načelom najmanjšega obsega podatkov, da so posnete tudi druge osebe v prostoru, zgolj zato, da bi se preprečilo prepisovanje. Šola mora s svojimi ukrepi v čim manjši meri posegati v zasebnost, da še zagotovi izpolnjevanje svojih nalog.

Treba je še poudariti, da mora upravljavec (šola) zagotavljati načeli vgrajenega in privzetega varstva osebnih podatkov tudi, ko ponudnike IT rešitev »najema« znotraj spletnih platform drugih ponudnikov. Zgolj dejstvo, da se določen ponudnik IT rešitve ponuja znotraj spletne platforme izbranega in preverjenega ponudnika (npr. ARNES, eAsistent), še ne zagotavlja skladnosti tega ponudnika.

Primer: ARNES za potrebe raziskovalcev in izobraževalnih zavodov na svoji platformi omogoča ponudbo komercialnih produktov različnih ponudnikov. Šola najame storitev, ki se ponuja prek te platforme, brez da bi jo preverila, saj meni, da jo je preveril že ARNES in jih priporoča. V inšpekcijskem nadzoru mora šola izkazati, da je izbranega ponudnika preverila in ustrezno uredila razmerja med njo kot upravljavcem, ARNESOM kot obdelovalcem in tretjim ponudnikom kot drugim obdelovalcem oziroma pod-obdelovalcem, kolikor gre za takšno situacijo (za dodatno razlago glej poglavje o pogodbeni obdelavi osebnih podatkov).

5 POGODBENA OBDELAVA IN SKUPNI UPRAVLJAVCI

5.1 Kdaj je pogodbeno obdelava ustrezno urejena - zahteve zakonodaje?

Pogodbena obdelava osebnih podatkov pomeni, da upravljavec (npr. šola) za določeno dejanje obdelave osebnih podatkov »najame« zunanjšega izvajalca – 'obdelovalca' (tudi *pogodbeni obdelovalec*). Obdelovalec deluje po navodilih upravljavca in v njegovem imenu obdela osebne podatke. Primer je oblačna hramba osebnih podatkov pri izbranem ponudniku (npr. Arnes, Logitus). Šola je *upravljavec* osebnih podatkov, ponudnik storitve oblačne hrambe pa *obdelovalec* osebnih podatkov.

Med upravljavcem in obdelovalcem **mora biti sklenjena pisna pogodba o obdelavi osebnih podatkov**, ki mora obvezno vsebovati vse elemente iz člena 28 Splošne uredbe. V skladu s členom 28(7) Splošne uredbe je IP pripravil tudi standardna pogodbeno določila, ki se lahko uporabijo kot **vzorčna pogodba** za ureditev razmerja med upravljavcem in obdelovalcem.²⁰ Pisna pogodba mora biti sklenjena tudi v primeru, ko je IT rešitev, ki jo uporablja upravljavec, brezplačna (npr. Google drive).

Dodati še velja, da standardna pogodbeno določila za pogodbo o obdelavi osebnih podatkov ne gre zamenjevati s »*standardnimi pogodbenimi klavzulami*« v skladu s členom 46(2)(c) in (d), ki so eden od možnih mehanizmov za prenos osebnih podatkov v tretje države (glej tudi poglavje 6 teh smernic).

→ Več o tem: [Ali se lahko uporablja standardna pogodbeno določila?](#)²¹

Pravila varstva osebnih podatkov zahtevajo, da se **obdelava v imenu upravljavca izvaja samo pri obdelovalcih, ki zagotavljajo zadostna jamstva za**

izvedbo zaščitnih ukrepov na tak način, da obdelava izpolnjuje zahteve iz uredbe. Pri izbiri obdelovalca mora torej upravljavec biti pozoren in iskati takšnega obdelovalca, ki izpolnjuje zahteve iz Splošne uredbe.

Obdelovalec lahko osebne podatke **obdeluje samo po dokumentiranih navodilih upravljavca**. To za **upravljavca pomeni**, da mora v pogodbi natančno opredeliti, kako naj obdelovalec obdeluje osebne podatke – na primer tako, da opredeli dovoljeno in nedovoljeno ravnanje z osebnimi podatki, natančnejše postopke, način zavarovanja osebnih podatkov ipd.²² Prav tako je priporočljivo vključiti postopke in predloge za nadaljnja navodila v prilogo k osnovni pogodbi o obdelavi osebnih podatkov.²³ Za **pogodbenega obdelovalca** pa to pomeni, da ne sme obdelovati osebnih podatkov v nasprotju z dokumentiranimi navodili upravljavca, sicer se šteje, da deluje kot samostojni upravljavec osebnih podatkov. To velja tudi glede prenosov osebnih podatkov v tretje države.²⁴ Edina izjema, ki dovoljuje obdelovalcu obdelovati osebne podatke zunaj dogovorjenega obsega je, če tako od obdelovalca zahteva pravo države ali pravo Unije. V tem primeru, pa mora obdelovalec upravljavca o tem obvezno obvestiti. Če obdelovalec obdelave ne izvaja po dokumentiranih navodilih upravljavca, potem nastopa kot samostojni upravljavec in mora sam izkazati pravno podlago ter izpolniti druge obveznosti po Splošni uredbi (informiranje, zagotavljanje pravic, evidentiranje itd.).

Če upravljavec dovoli, lahko obdelovalec za obdelavo osebnih podatkov najame »pod-obdelovalca«, ki je v neposrednem pogodbenem razmerju z obdelovalcem. Dovoljenje je lahko **splošno** (za kateregakoli pod-obdelovalca) ali **posebno** (le za določene pod-obdelovalce ali le za določene dejavnosti obdelave). Upravljavec pa je v vsakem primeru dolžan izkazati, da je obdelovalcu podal dovoljenje za najem pod-obdelovalca (običajno je takšno dovoljenje priloga pogodbi o obdelavi). Če je dovoljenje splošno, mora biti

²⁰ https://www.ip-rs.si/fileadmin/user_upload/Pdf/Standardna_pogodbena_dolocila_-_clen_28_15jul2020.pdf

²¹ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/pogodbena-obdelava#pogodbenaDolocila>

²² Smernice EDPB 07/2020 glede pojmov upravljavec, obdelovalec in skupni upravljavec osebnih podatkov, z dne 7. 7. 2021, tč. 116 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en).

²³ Prav tam tč. 118.






²⁴ Prav tam tč. 119.

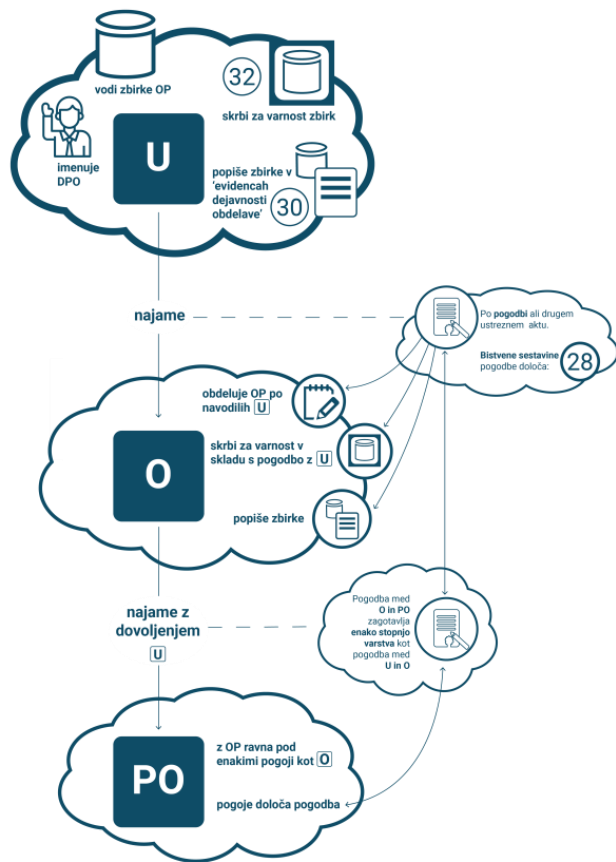
upravljavca obveščen o vseh nameranih spremembah pod-obdelovalcev in hkrati mora imeti možnost nasprotovati izbiri.²⁵ S tem se zagotovi, da upravljavca dejansko obvladuje celoten cikel obdelave osebnih podatkov (pri vseh deležnikih, vključno z vsemi pod-obdelovalci osebnih podatkov). V praksi, zlasti pri internetnih storitvah, je veriga obdelovalcev in pod-obdelovalcev lahko zelo kompleksna – tudi do več deset ravni pod-obdelovalcev, ki na primer zagotavljajo storitev strežniškega prostora, vzdrževanje idr. Za lažjo predstavo sistema si oglejte spodnjo shemo.

Več o pogodbeni obdelavi:

- ➔ Infografika: [Infografika o pogodbeni obdelavi](#)²⁶
- ➔ Spletna stran IP: [Pogodbena obdelava](#)²⁷
- ➔ Smernice IP: [Smernice o \(pogodbeni\) obdelavi osebnih podatkov po Splošni uredbi o varstvu podatkov](#)²⁸
- ➔ [Smernice EDPB 07/2020 glede pojmov upravljavca, obdelovalec in skupni upravljavca osebnih podatkov, z dne 7. 7. 2021](#)²⁹

LEGENDA

-  posameznik
-  upravljavca
-  obdelovalec
-  (pod)obdelovalec
-  člen Splošne uredbe (GDPR)
-  osebni podatek



Upravljavca mora obvladovati celoten proces obdelave osebnih podatkov, ki jih izvaja sam ali jih zanj izvajajo pogodbeni obdelovalci in morebitni pod-obdelovalci.

²⁵ Prav tam, tč. 152.

²⁶ https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/INFOGRAFIKA_Pogodbena_obdelava_1_.pdf

²⁷ <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/pogodbena-obdelava#pogodbenaDolocila>

²⁸ <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-o-pogodbeni-obdelavi>

²⁹ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

5.2 Skupni upravljavci osebnih podatkov

Splošna uredba skupne upravljavce definira kot dva ali več upravljavcev, ki **skupaj določijo namene in načine obdelave** (člen 26 Splošne uredbe). Gre za institut Splošne uredbe, ki omogoča, da se uredijo razmerja, ko želita dva ali več subjektov izvajati isti projekt ali sledita istemu cilju, pri katerem pride do obdelave osebnih podatkov. To so na primer *skupne informacijske baze, skupna ureditev in uporaba določene infrastrukture (spletne platforme), dogodki in prireditve z več organizatorji ipd.*

Pri skupnih upravljavcih je pomembno, da *namene in načine* obdelave **določijo skupno**. Ni potrebno, da vse obdelave izvajajo vsi upravljavci oziroma, da vsak podatke obdeluje za isti namen – morajo pa namene predhodno skupno določiti. Tudi ni potrebno, da ima vsak upravljavec nadzor nad vsemi stopnjami konkretne obdelave. Lahko so posamezni skupni upravljavci vključeni v različne stopnje konkretne obdelave osebnih podatkov in v različnem obsegu.

Za **razliko od pogodbene obdelave** skupni upravljavci ne delujejo po samovoljnih in izključnih navodilih enega ali drugega. Skupni upravljavci se v medsebojnem dogovoru dogovorijo, kako bodo obdelovali osebne podatke. Ključna razlika s pogodbeno obdelavo je tudi v tem, da skupna upravljavca še vedno nastopata kot upravljavca, torej da za obdelavo zagotavljata vsak svojo ustrezno pravno podlago (pri pogodbeni obdelavi

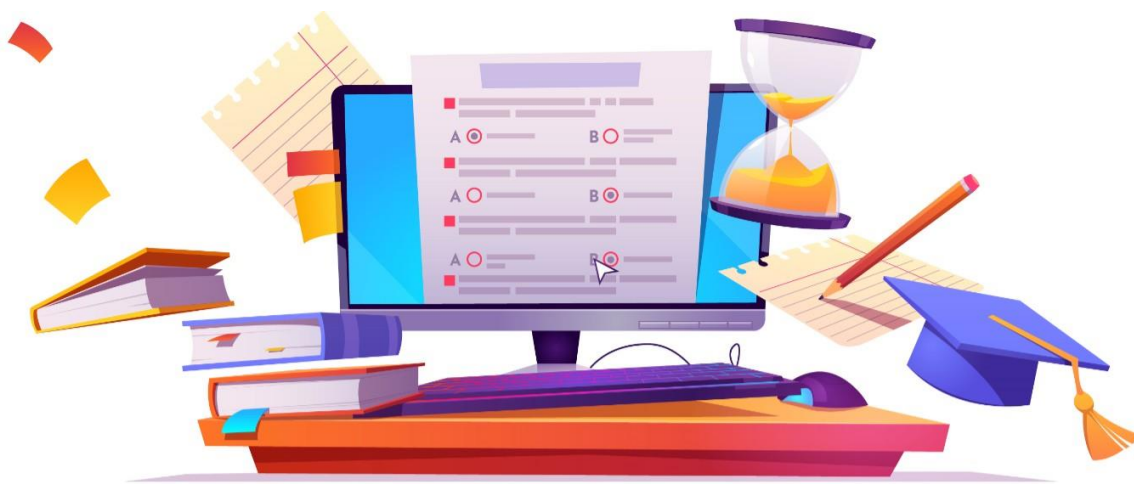
pravni temelj obdelovalcu zagotavlja ustrežna pogodba z upravljavcem).

Pri skupnih upravljavcih je ključnega pomena, da so **obveznosti do posameznikov enake, kot če bi bil le en upravljavec**. Posameznik lahko namreč pri vsakem upravljavcu izvršuje vse svoje pravice po Splošni uredbi v zvezi s skupno obdelavo, ne glede na to, ali dotični upravljavec tudi izvaja konkretno obdelavo v zvezi s katero prejme zahtevo posameznika.

Vlogo in naloge pri skupni obdelavi skupni upravljavci določijo v **medsebojnem dogovoru**. Vsebine tega dogovora Splošna uredba ne ureja tako natančno, kot ureja pogodbo pri pogodbeni obdelavi (člen 28). IP je zato pripravil **priporočila**, ki vsebujejo tudi okvirni seznam sestavin, ki bi jih moral vsebovati medsebojni dogovor, da se zagotovi skladnost s Splošno uredbi.

Več o skupnih upravljavcih:

- ➔ [Priporočila Informacijskega pooblaščenca glede skupnih upravljavcev](#)³⁰
- ➔ [Infografika: Skupni upravljavci](#)³¹
- ➔ [Smernice EDPB 07/2020 glede pojmov upravljavec, obdelovalec in skupni upravljavec osebnih podatkov, z dne 7. 7. 2021](#)



³⁰ https://www.ip-rs.si/dokumenti/razno/Priporocila_Informacijskega_Pooblasčenca_glede_s_kupnih_upravljavcev_21jan2019.pdf

³¹ <https://www.ip-rs.si/publikacije/infografike>

6 PRENOSI V TRETJE DRŽAVE IN MEDNARODNE ORGANIZACIJE

6.1 Kdaj gre za prenos?

O prenosu osebnih podatkov v tretje države ali mednarodne organizacije govorimo takrat, ko upravljavec ali obdelovalec iz Slovenije ali druge države članice Evropske unije (izvoznik podatkov) osebne podatke posreduje v države izven Evropskega gospodarskega prostora (EGP; sem sodijo poleg držav EU tudi Islandija, Norveška in Lihtenštajn) ali mednarodni organizaciji (uvoznik podatkov). O prenosu govorimo tudi takrat, ko je dostop do osebnih podatkov omogočen organizacijam, podjetjem, posameznikom ali drugim subjektom iz tretjih držav izven EGP, pa čeprav so podatki hranjeni znotraj EGP.

6.2 Pod kakšnimi pogoji je prenos dopusten?

Namen določb o prenosu podatkov v tretje države in mednarodne organizacije je **zagotavljanje enake ravni varstva osebnih podatkov** za podatke, ki se obdelujejo znotraj EU, in tiste, ki so posredovani v tretje države, ter tudi tiste, ki so nadalje posredovani iz tretje države ali mednarodne organizacije v druge tretje države in v druge mednarodne organizacije.

Za zakonito obdelavo osebnih podatkov, ki se prenašajo v tretjo državo, mora:

(1.) obstajati ustrezna pravna podlaga za obdelavo osebnih podatkov v skladu s členom 6(1) Splošne uredbe, torej za posredovanje osebnih podatkov od izvoznika k uvozniku podatkov - pri prenosu podatkov od upravljavca k obdelovalcu je treba upoštevati pogoje iz člena 28 Splošne uredbe o varstvu podatkov ter v skladu s tem skleniti pogodbo o obdelavi osebnih podatkov, pri prenosu od upravljavca k drugemu upravljavcu pa mora za tako posredovanje obstajati ustrezna pravna podlaga;

(2.) dodatno morajo biti zagotovljeni pogoji za prenos osebnih podatkov v tretjo državo (zagotovljena mora biti ustrezna raven varstva podatkov).

Ustrezna raven varstva osebnih podatkov po prenosu je lahko zagotovljena na več načinov, v praksi, v zvezi z uporabo IT rešitev v šolstvu, pa bosta najpogostejša naslednja mehanizma, pri katerih **se ne zahteva predhodne odobritve s strani IP**:

- (1) če za uvoznika v tretji državi velja, da zagotavlja ustrezno raven varstva osebnih podatkov – **to določi Evropska Komisija s t.i. sklepom o ustreznosti**. V času izdaje predmetnih smernic navedeno velja za *Andoro, Argentino, Kanada, Ferske otoke, Guernsey, Izrael, Isle of Man, Jersey, Severno Makedonijo, Novo Zelandijo, Švico, Urugvaj, Japonsko in Združeno kraljestvo*.
- (2) z uporabo tipskega besedila pogodb, ki jih je pripravila Evropska komisija – **standardne pogodbene klavzule (SPK), ki so bile spremenjene in sprejete dne 4.6.2021, pričele pa so veljati 27.6.2021** ([Uradni list EU L 199 dne 7. junija 2021](#)³²). V primeru prenosa osebnih podatkov na podlagi SPK mora šola po potrebi zagotoviti tudi dopolnilne zaščitne ukrepe, ki zagotavljajo varovanje zasebnosti ter temeljnih človekovih pravic na enaki ravni, kot je to zagotovljeno v okviru EU.

Primer: Šola uporablja storitev Zoom za izvajanje pouka na daljavo. Obdelovalec je ponudnik storitve. Da bi šola delovala skladno s predpisi s področja varstva osebnih podatkov, mora s ponudnikom (obdelovalcem):

1. skleniti ustrezno pogodbo o obdelavi osebnih podatkov v skladu s členom 28 Splošne uredbe (uporabi lahko tudi [Standardna pogodbena določila](#)³³) IN
2. preveriti, ali pride do prenosa osebnih podatkov v tretje države, ki niso zajete v seznamu držav ali ozemelj, za katere velja *sklep o ustreznosti* (npr. ZDA niso pokrite s

³² <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=OJ:L:2021:199:TOC>

³³ https://www.ip-rs.si/fileadmin/user_upload/Pdf/Standardna_pogodbena_dolocila_-_clen_28_15jul2020.pdf

sklepom o ustreznosti). V takem primeru mora šola zagotoviti ustrezen drug temelj za prenos, npr. da s ponudnikom sklene »standardne pogodbene klavzule« ([Uradni list EU L 199 dne 7. junija 2021](#)), pri čemer morajo biti po potrebi vzpostavljeni tudi ustrezni dopolnilni zaščitni ukrepi, ki zagotavljajo varovanje zasebnosti ter temeljnih človekovih pravic na enaki ravni, kot je to zagotovljeno v okviru EU.

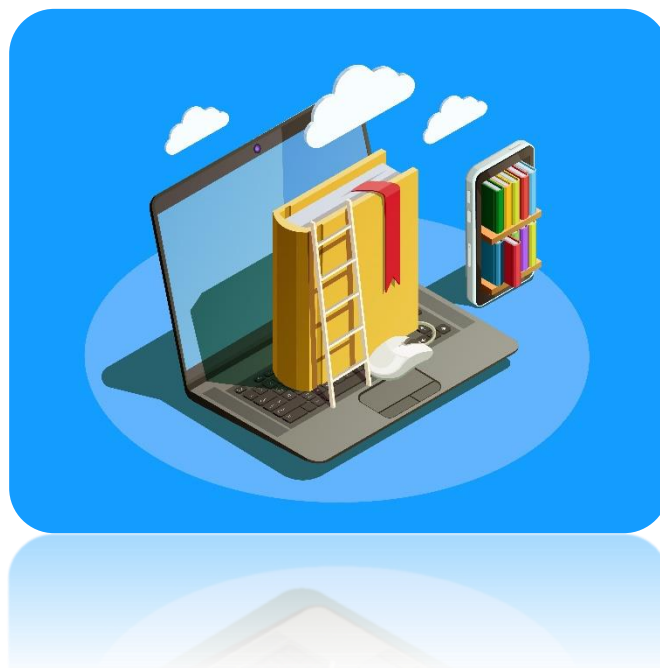
3. Ko šola zagotovi podlago za prenos, mora o tem obvestiti tudi posameznike, katerih osebne podatke obdeluje (učenci, zaposleni, starši...). V skladu s členom 13(1)(f) Splošne uredbe, mora upravljavec v informacije vključiti tudi »sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo«.

Treba je dodati, da enako, kot smo v primeru opisali za platformo Zoom, velja tudi za druge IT rešitve, kjer pride do prenosa osebnih podatkov v tretje države – npr. Google Drive ali Office 365.

Več o tem:

- Smernice IP: [Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije po Splošni uredbi o varstvu podatkov](#)³⁴
- Novica IP: [Veljati so začele nove standardne pogodbene klavzule za prenos osebnih podatkov v tretje države](#)³⁵
- Infografika: [Prenos osebnih podatkov po Splošni uredbi v tretje države in mednarodne organizacije v dveh korakih](#)³⁶

Ker so pogoji za zakonit prenos pravno in tehnološko zahtevni, bo v praksi nujno, da šole glede uporabe posameznih IT rešitev, ki omogočajo zakonit prenos osebnih podatkov v tretje države, pristopijo enotno, ob ustrezni strokovni podpori tako pravne kot tudi informacijsko-tehnološke stroke. V vsakem primeru je odsvetovano »samostojno« ravnanje učiteljev pri izbiri IT rešitev, saj so tveganja za nezakonito obdelavo osebnih podatkov v teh primerih visoka, za skladno obdelavo pa je odgovoren upravljavec osebnih podatkov (to je šola).



³⁴ <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-glede-prenosa-osebni-podatkov-v-tretje-dr%C5%BEave-in-mednarodne-organizacije-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov>

³⁵ <https://www.ip-rs.si/novice/veljati-so-za%C4%8Dele-nove-standardne-pogodbene-klavzule-za-prenos-osebni-podatkov-v-tretje-dr%C5%BEave>

³⁶ https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Prenos_osebni_podatkov_v_dveh_korakih.pdf

7 INFORMIRANJE IN PRAVICE

7.1 Informiranje posameznikov (členi 12 -14 Splošne uredbe)

7.1.1 Zakaj je treba posameznike obvestiti o tem, da se njihove osebne podatke obdeluje?

Ker je to pošteno. Ker se mora posameznik zavedati obdelave njegovih osebnih podatkov, da lahko svojo pravico do varstva osebnih podatkov uresničuje. Za posameznika namreč pomenijo ustrezne, pravočasne in razumljive informacije to, da lahko uveljavlja svoje pravice po Splošni uredbi (zahteva dostop do informacij v zvezi z obdelavo, zahteva popravek osebnih podatkov, obdelavi svojih podatkov ugovarja ipd). Predpogoj skladne obdelave osebnih podatkov je torej, da se posameznik zaveda obdelave njegovih osebnih podatkov, saj lahko le tako pričakuje posledice takšne obdelave in posledično tudi v določeni meri vpliva na to, kaj se bo z njegovimi osebnimi podatki dogajalo.

Informiranje posameznikov je ključno za pravico do varstva osebnih podatkov in zagotavlja pošteno obdelavo osebnih podatkov. Zato Splošna uredba **upravljavcem nalaga obveznost**, da informirajo posameznike o vseh pomembnih vidikih obdelave osebnih podatkov. Opustitev informiranja je lahko dopustna le izjemoma, in sicer ko to izrecno predpisuje zakon. Nekateri izjeme glede obveznosti informiranja vsebuje že Splošna uredba (člena 13(4) in 14(5) Splošne uredbe) – več o tem v nadaljevanju.

7.1.2 Katere informacije mora upravljavec sporočiti posamezniku?

Upravljavci morajo posameznike informirati glede vseh informacij, ki jih zahtevata člena 13(1) in (2) ter člen 14(1) in (2) Splošne uredbe. Posredovati mu morajo informacije, kot so:

- **Kdo** je upravljavec? (naziv, sedež, kontaktni podatki)
- **Zakaj** obdeluje osebne podatke? (NAMEN in PRAVNA PODLAGA)

- **Komu** bo podatke **posredoval**? (morebitni OBDELOVALCI, drugi UPRAVLJACI ali UPORABNIKI in če bo podatke posredoval v tretje države)
- **Koliko časa** bo upravljavec podatke hranil?
- **Katere** so posameznikove **pravice**? (posebej o pravici do ugovora)
- **Ali namerava zbrane podatke (za osnovni namen) uporabiti še za drug namen?**

Kadar upravljavec osebnih podatkov ne zbira od posameznika, mu mora poleg zgoraj navedenih informacij posredovati še informacije o:

- **vrsti osebnih podatkov**, ki jih je pridobil,
- **od kje izvirajo** osebni podatki in po potrebi, ali izvirajo iz javno dostopnih virov.

Preden upravljavec prične z informiranjem posameznikov, mora jasno ugotoviti za kakšen namen in na kateri pravni podlagi zbira osebne podatke. To je ključno za zakonitost obdelave osebnih podatkov. Ob zbiranju osebnih podatkov pa mora te in druge informacije posredovati posamezniku. Navedeno velja za vse osebne podatke, ki jih upravljavec zbira (npr. tudi telefonske številke in elektronske naslove staršev otrok).

Kadar upravljavec ugotovi, da mora osebne podatke zbirati na podlagi člena 6(1)(e) Splošne uredbe (za izvajanje javne oblasti ali za izvajanje naloge v javnem interesu) ali člena 6(1)(f) Splošne uredbe (za zakonite interese), mora posamezniku ob zbiranju jasno razvidno in **ločeno od ostalih informacij posredovati tudi informacijo o pravici do ugovora**. Na ta način se zagotovi posamezniku možnost, da nasprotuje obdelavi njegovih osebnih podatkov, upravljavec pa mora osebne podatke prenehati obdelovati za ta namen, razen če izkaže nujne legitimne razloge za obdelavo (več o tem pri pravici do ugovora).

Velja dodati, da si mora upravljavec (že ob zbiranju) zabeležiti **iz katerih virov** je podatke pridobil. Z virom pridobljenih informacij mora namreč upravljavec (proaktivno) seznaniti posameznike skladno s členom 14(2)(f). Posameznik pa lahko informacije o viru tudi

zahteva, in sicer v skladu s pravico dostopa do lastnih osebnih podatkov na podlagi člena 15(1)(g) Splošne uredbe.

Natančne informacije, ki jih je upravljavec dolžan posredovati so opredeljene tudi v Obrazcih IP (glej spodaj). Podrobna razlaga posamezne kategorije informacij, ki jih mora upravljavec posredovati posamezniku, izhaja iz evropskih [Smernic o preglednosti na podlagi Uredbe \(EU\) 2016/679, nazadnje revidirane in sprejete 11. aprila 2018](#)³⁷

Obrazca IP:

- [Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 13 Splošne uredbe\)](#)³⁸
- [Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 14 Splošne uredbe\)](#)³⁹

7.1.3 Kako morajo biti informacije podane?

Poleg vsebine informacij, ki jih mora upravljavec (šola) sporočiti, pa je po Splošni uredbi zelo pomembno tudi, da so posamezniki obveščeni **na razumljiv in pregleden način** – tako, da so informacije prilagojene tipičnemu posamezniku, ki so mu informacije namenjene. Informiranje je za upravljavca obvezno do vseh posameznikov, ne glede na to v kakšnem razmerju nastopa do njih. Šola kot upravljavec mora torej informirati tako učence/dijake (in njihove starše, ko so otroci mlajši od 15 let), kot tudi svoje zaposlene (npr. učiteljice in učitelje, katerih osebni podatki se obdelujejo).

7.1.4 Kdaj je treba posameznike informirati?

Ko se osebne **podatke zbira neposredno od posameznika**, velja obveznost po členu 13 Splošne uredbe in **je informacije treba podati najkasneje ob zbiranju**. V primeru uporabe IT rešitev to na primer

pomeni, da morajo biti posamezniki informirani o namenu, pravni podlagi in drugih pomembnih informacijah v zvezi z uporabo IT rešitve, **ob zbiranju osebnih podatkov (npr. ko šola pridobi e-naslov ali telefonsko številko) in pred uporabo aplikacije, storitve itd.**

Posameznik se mora v trenutku, ko posreduje svojo telefonsko številko ali e-naslov zavedati za kakšen namen, na kateri pravni podlagi, komu in za koliko časa posreduje svoje osebne podatke in kakšne so njegove pravice. Te informacije morajo biti posamezniku posredovane, ko upravljavec podatke od posameznika zbira.

Kadar je potrebna namestitev določene programske opreme na zasebne naprave, potem morajo biti informacije podane pred namestitvijo, hkrati pa mora posameznik s takšno namestitvijo tudi podati svojo privolitev (glej zgoraj – privolitev v zvezi z 157. členom ZEKom-1). Ob tem velja izpostaviti, da privolitev za obdelavo osebnih podatkov ni podana že s tem, ko je posameznik z obdelavo seznanjen. Za veljavno privolitev je potrebna aktivnost posameznika (npr. obkljukanje kvadratka pred »strinjam se«, podaja pisne izjave itd). Po drugi strani pa je obveznost informiranja (ki izhaja iz členov 13 in 14 Splošne uredbe), širša od zbiranja privolitev. V nekaterih primerih bo osebne podatke posameznik moral posredovati, ker tako določa zakon. Tudi v tem primeru pa mora upravljavec (šola) posameznika seznaniti z vsemi potrebnimi informacijami, po členih 13 oziroma 14 Splošne uredbe.

Če upravljavec osebnih podatkov **ne zbira neposredno od posameznikov** pač pa **iz drugih virov** (tretji upravljavci podatkov, javni viri, posredniki podatkov ali

³⁷ <https://ec.europa.eu/newsroom/article29/items/622227>

³⁸ https://www.ip-rs.si/fileadmin/user_upload/doc/vzorci/VZOREC_OBVESTILA_P_OSAMEZNIKOM_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx

³⁹ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/OBVESTILO_POSAMEZNIK_OM_PO_14._CLENU_SPLOSNE_UREDBE_O_VARSTVU_PODATKOV_GDPR_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx

drugi posamezniki), **mora podati informacije v rokih iz člena 14(3) Splošne uredbe**. V tem primeru **na splošno** velja, da mora upravljavec informacije posredovati v razumnem roku po prejemu osebnih podatkov, vendar **najpozneje v enem mesecu**. Upoštevajo pa se tudi določene posebne okoliščine, in sicer:

- **Splošni enomesečni rok se skrajša**, če se osebni podatki uporabijo za komuniciranje s posameznikom, na katerega se nanašajo osebni podatki. V tem primeru je treba informacije zagotoviti **najpozneje ob prvem komuniciranju s posameznikom, ne pa kasneje** (če je prvo komuniciranje kasneje kot v enem mesecu od zbiranja osebnih podatkov, je treba posameznike obvestiti v enomesečnem roku).
- Splošni enomesečni rok **se skrajša tudi** na podlagi člena 14(3)(c), **če je predvideno razkritje drugemu uporabniku** (ki je tretja oseba ali ne). V tem primeru je treba informacije zagotoviti najpozneje ob prvem razkritju.

7.1.5 Kdaj posameznikov ni treba obveščati?

Omenili smo že, da lahko izjeme od obveznosti informiranja predpiše samo zakon, ki sledi taksativno določenim ciljem zapisanim v členu 23 Splošne uredbe.

Splošna uredba v členu 13(4) ureja izjemo od obveznosti informiranja v primeru, ko se osebne podatke zbira neposredno od posameznika, na katerega se osebni podatki nanašajo – in sicer določa, da **posameznika ni treba obveščati, kadar informacije že ima.**

Po mnenju IP zgolj dejstvo, da je obdelava predpisana z zakonom še ne pomeni, da posameznik (zaradi publicitete predpisa) že ima informacije o obdelavi osebnih podatkov in ga zato ne bi bilo treba obveščati. **Tudi, ko se podatke zbira na podlagi zakona, mora upravljavec informacije posredovati, razen kadar zakon izrecno določa, da informiranje ni potrebno.**

Kadar pa se osebnih podatkov ne zbira od posameznika (člen 14 Splošne uredbe), je določen obsežnejši nabor izjem od obveznosti obveščanja, ki veljajo za upravljavca podatkov, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo osebni podatki. Splošno pravilo je, da bi bilo treba te izjeme razlagati in uporabljati ozko. Poleg okoliščin, v katerih posameznik, na katerega se nanašajo osebni podatki, že ima zadevne informacije (člen 14(5)(a)), so v skladu s členom 14(5) določene še naslednje izjeme:

- **zagotavljanje takih informacij je nemogoče** ali bi vključevalo nesorazmeren napor, zlasti pri obdelavi v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene,
- za **upravljavca velja zahteva iz nacionalnega prava** ali prava EU, **v skladu s katero mora pridobiti ali razkriti osebne podatke**, pri čemer so v skladu s pravom določeni ustrezni zaščitni ukrepi za zakonite interese posameznika, na katerega se nanašajo osebni podatki, ali
- osebni podatki **morajo ostati zaupni zaradi obveznosti varovanja poklicne skrivnosti** (vključno s statutarno obveznostjo varovanja skrivnosti) v skladu z nacionalnim pravom ali pravom EU.

➔ Več informacij o posameznih izjemah od obveznosti obveščanja po členu 14(5) Splošne uredbe najdete v [Smernice o preglednosti na podlagi Uredbe \(EU\) 2016/679, nazadnje revidirane in sprejete 11. aprila 2018](#),⁴⁰ str. 30 in naslednje.

Več o pregledni obdelavi osebnih podatkov:

- ➔ Obrazec IP: [Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 13 Splošne uredbe\)](#)
- ➔ Obrazec IP: [Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 14 Splošne uredbe\)](#)⁴¹

⁴⁰ <https://ec.europa.eu/newsroom/article29/items/622227>

⁴¹ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/OBVESTILO_POSAMEZNIK

- Spletna stran tiodlocas.si⁴²
- [Smernice o preglednosti na podlagi Uredbe \(EU\) 2016/679, nazadnje revidirane in sprejete 11. aprila 2018](#)⁴³

- [Zahteva za seznanitev z lastnimi osebnimi podatki \(obrazec SLOP\)](#)⁴⁶
- [Pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki \(obrazec P-SLOP\)](#)⁴⁷

7.2 Pravice posameznikov (členi 15 – 22 Splošne uredbe)

Splošna uredba omogoča posameznikom uresničevanje njihovih pravic pri upravljalcih osebnih podatkov. Če na primer posameznik zahteva dostop ali izbris svojih osebnih podatkov, se upravljaivec ne more izogniti odločanju z utemeljitvijo, da podatke zanj obdeluje obdelovalec, ki ima sedež v tretji državi in da zato nanj nima vpliva. Sklepanje podrobnih pogodb z obdelovalci se po zakonodaji zahteva prav zato, da bi posamezniki imeli možnost učinkovitega varstva svojih pravic, tudi ko njihove osebne podatke obdeluje obdelovalec, ki je na primer organizacija iz ZDA.

- **Pravice, ki jih lahko uveljavljajo posamezniki so naslednje:**

- **PRAVICA DO DOSTOPA ALI DO SEZNANITVE Z LASTNIMI OSEBNIMI PODATKI (ČLEN 15);** omogoča posamezniku, da od upravljalca zahteva **določene informacije** v zvezi z obdelavo njegovih osebnih podatkov IN **tudi vpogled** oziroma **pridobitev kopije** posameznikovih osebnih podatkov.

Več o pravici dostopa:

- spletna stran tiodlocas.si: [Želim vedeti, kaj počnejo z mojimi podatki](#)⁴⁴
- Spletna stran IP: [Seznanitev z lastnimi osebnimi podatki ali pravica do dostopa do osebnih podatkov](#)⁴⁵

OBRAZCI:

- **PRAVICA DO POPRAVKA (ČLEN 16);** omogoča posamezniku, da zahteva **popravek netočnih ali neažurnih podatkov** v zvezi z njim in **dopolni nepopolne** osebne podatke.

Več o pravici do popravka:

- Spletna stran tiodlocas.si: [Želim popraviti netočne podatke](#)⁴⁸

Pomembno je, da se šole kot upravljalci zavedajo, da morajo posameznike od katerih zbirajo osebne podatke (npr. učence oziroma njihovi starše/skrbnike in zaposlene), pred pričetkom obdelave njihovih osebnih podatkov obvestiti o vseh okoliščinah v zvezi z obdelavo osebnih podatkov – to velja tudi na primer, ko se za izvajanje pouka uporablja IT rešitev, kot smo že opisali zgoraj.

- **PRAVICA DO IZBRISA** (pravica do POZABE) (ČLEN 17); omogoča posamezniku, da pod določenimi pogoji zahteva izbris svojih osebnih podatkov. Pravica do izbrisa ni absolutna, temveč lahko pride v poštev le pod pogoji, ki jih določa člen 17(1) Splošne uredbe, in sicer:
 - (a) osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;

OM PO 14. ČLENU SPLOŠNE UREDBE O VARSTVU PODATKOV GDPR
GLEDE OBDELAVE OSEBNIH PODATKOV.docx

⁴² Transparentna obdelava osebnih podatkov, <https://tiodlocas.si/moram-biti-obvescen/>.

⁴³ <https://ec.europa.eu/newsroom/article29/items/622227>

⁴⁴ https://tiodlocas.si/?page_id=106

⁴⁵ <https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/seznanitev-z-lastnimi-osebnimi-podatki/>

⁴⁶ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva_za_seznanitev_z_lastnimi_osebnimi_podatki_Obrazec_SLOP.doc

⁴⁷ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Pritožba_zaradi_kršitve_pravice_do_seznanitve_z_lastnimi_osebnimi_podatki_Obrazec_P-SLOP.doc

⁴⁸ <https://tiodlocas.si/zelim-popraviti-netocne-podatke/>

- (b) posameznik, na katerega se nanašajo osebni podatki, prekliče privolitve, na podlagi katere poteka obdelava v skladu s točko (a) člena 6(1) ali točko (a) člena 9(2), in kadar za obdelavo ne obstaja nobena druga pravna podlaga;
- (c) posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja v skladu s členom 21(1), za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi, ali pa posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja v skladu s členom 21(2);
- (d) osebni podatki so bili obdelani nezakonito;
- (e) osebne podatke je treba izbrisati za izpolnitev pravne obveznosti v skladu s pravom Unije ali pravom države članice, ki velja za upravljavca;
- (f) osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe iz člena 8(1).

Primer (umik privolitve): šola je na svoji FB strani objavila fotografije in dosežke učencev na regijskem tekmovanju. Objavo je izvedla na podlagi privolitve, ki so bile zbrane na začetku šolskega leta. Nekateri starši niso želeli, da se podoba njihovih otrok razširja po socialnih omrežjih, zato so privolitve umaknili in zahtevali izbris objav.

Primer (osebni podatki niso več potrebni v namene, za katere so bili zbrani): 98. člen ZOsn določa, da se zbirke podatkov o učencu, napredovanju, izdanih spričevalih in drugih listinah hranijo trajno, ostali podatki iz zbirk podatkov, ki jih vodi osnovna šola, pa se hranijo eno leto po zaključku šolanja učenca. Posameznik lahko zahteva izbris podatkov, ki bi jih šola hranila dalj časa, kot je določen zakonski rok hrambe.

Več o pravici do izbrisa (pravici do pozabe):

- ➔ spletna stran tiodlocas.si: [Želim izbrisati svoje podatke](https://tiodlocas.si/zelim-izbrisati-svoje-podatke/)⁴⁹
- ➔ spletna stran tiodlocas.si: Izbris osebnih podatkov in pravica do pozabe⁵⁰

- **PRAVICA DO OMEJITVE OBDELAVE (ČLEN 18);** omogoča posamezniku, da zahteva, da upravljavec ne izbriše podatkov temveč zgolj omeji obdelavo (podatkov ne obdeluje več, jih pa še vedno hrani). Pravica do omejitve obdelave lahko pride v poštev na primer, ko bi bil posameznik sicer upravičen zahtevati izbris, pa vseeno želi, da upravljavec podatke hrani zaradi morebitnih kasnejših dokazovanj pred pristojnimi organi ali drugimi deležniki. Prav tako lahko pravica pride v poštev, če posameznik zahteva, da upravljavec podatkov ne zbriše, ko bi jih glede na predviden rok hrambe sicer zbrisal, zaradi uveljavljanja svojih pravnih zahtevkov (npr. posnetek, ki ga je učenec posedoval in na podlagi katerega je bil ocenjen, pa želi svojo oceno izpodbijati v predvidenem postopku in zahteva, da šola do zaključka vseh postopkov posnetka ne izbriše).

Več o pravici do omejitve obdelave:

- ➔ Spletna stran tiodlocas.si: [Želim omejiti obdelavo svojih podatkov](https://tiodlocas.si/zelim-omejiti-obdelavo-svojih-podatkov/)⁵¹

- **PRAVICA DO PRENOSLJIVOSTI (ČLEN 20);** Omogoča posamezniku, da zahteva od upravljavca, da posreduje drugemu upravljavcu (ali posamezniku) osebne podatke, ki jih vodi o tem posamezniku v strojno berljivi obliki. Pogoji so, da upravljavec podatke obdeluje z avtomatiziranimi sredstvi in na podlagi privolitve oziroma zaradi pogodbe. Dodati velja, da se skladno z izrecno določbo Splošne uredbe ta pravica »ne uporablja za obdelavo, potrebno za opravljanje naloge, ki se izvaja v javnem

⁴⁹ <https://tiodlocas.si/zelim-izbrisati-svoje-podatke/>

⁵⁰ <https://tiodlocas.si/top-nasveti/izbris-osebni-podatkov-in-pravica-do-pozabe/>

⁵¹ <https://tiodlocas.si/zelim-zacasno-zamrzniti-svoje-podatke/>

interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu«. Glede na navedeno šolam, ki izvajajo izobraževanje kot javno službo, ni treba odločati o prenosljivosti, če se zahteva nanaša na osebne podatke v zvezi z izobraževanjem.

Več o pravici do prenosljivosti:

→ Spletna stran tiodlocas.si: [Želim prenesti svoje podatke k sebi ali k drugim upravljavcem](https://tiodlocas.si/zelim-prenesti-svoje-podatke-k-sebi-ali-k-drugim-upravljavcem)⁵²

- **PRAVICA DO UGOVORA (ČLEN 21)**; omogoča posameznikom, da ugovarjajo obdelavi, ki se izvaja na podlagi zakonitih interesov (na podlagi člena 6(1)(f) Splošne uredbe; velja za zasebni sektor) ali zaradi izvajanja naloge v javnem interesu ali javne oblasti (na podlagi člena 6(1)(e) Splošne uredbe; velja za javni sektor). Če posameznik ugovarja obdelavi, mora upravljavec prenehati z obdelavo, razen če dokaže nujne legitimne razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov. Pravica do ugovora je pomemben gradnik za vzpostavitev ravnotežja med pravico posameznika in interesom upravljavca. Z uveljavljanjem pravice do ugovora ima posameznik namreč možnost, da nasprotuje obdelavi svojih osebnih podatkov, v katero ni predhodno privolil ali se k njej zavezal zaradi sklenitve pogodbe. Podlaga za izvajanje obdelave osebnih podatkov po točki (f) ali (e) sloni na lastni oceni zakonitosti, ki jo izvede upravljavec. Z uveljavljanjem ugovora pa lahko posameznik nasprotuje skladnosti te ocene in iz tega razloga zahteva prenehanje obdelave. Ker po naravi pravnih podlag po točkah (f) ali (e), posameznik nima možnosti »predhodno odobriti« obdelave, je zelo pomembno, da so posamezniki o obdelavi na **primeren način tudi obveščeni**. Pravica do ugovora skupaj z

obvestilom daje posamezniku vsaj določeno mero vpliva nad tem, kaj se dogaja z njegovimi osebnimi podatki. Informacija o pravici do ugovora mora biti posamezniku podana istočasno, kot vse ostale informacije – mora pa biti **jasno razločna od drugih informacij**. Posameznik pa mora biti jasno in razločno informiran tudi o razlogih oz. interesu, ki utemeljuje obdelavo osebnih podatkov.

Pravica do ugovora torej daje posamezniku možnost, da ugovarja obdelavi, upravljavec pa mora takoj prenehati izvajati obdelavo, razen če dokaže, da obstajajo '**nujni legitimni razlogi za obdelavo**'. Kdaj bo nujno, da se obdelavo izvaja, bo odvisno od konkretnih primerov, pri tem pa je treba poudariti, da mora upravljavec dokazati, da obstajajo takšni razlogi, zaradi katerih lahko utemeljeno zavrne ugovor. Obrazložitev upravljavca mora biti konkretna in ustrezno upoštevati razloge, ki jih navaja posameznik v svojem ugovoru.

V šolstvu zlasti v zvezi z uporabo IT rešitev, ko ni jasnih zakonskih določb, ki bi urejale, katere osebne podatke in za katere namene mora šola osebne podatke obdelovati, bo podlaga za obdelavo osebnih podatkov po členu 6(1)(e) verjetno pogosto prišla v poštev. Kadarkoli pa upravljavec obdeluje osebne podatke na tej pravni podlagi, mora nujno imeti v mislih tudi pravico do ugovora, ki predstavlja garant zakonite obdelave, in o tej pravici ločeno obvestiti posameznike pred pričetkom obdelave osebnih podatkov.

Poseben režim je predviden za **neposredno trženje** - v tem primeru mora upravljavec takoj prenehati z obdelavo in ugovora ne more zavrniti. Poseben režim velja tudi za obdelave z **znanstveno- ali zgodovinskoraziskovalnim ali statističnim namenom**. V tem primeru

⁵² <https://tiodlocas.si/zelim-prenesti-svoje-podatke/>

posameznik z ugovorom ne more uspeti, če se ta namen izpolnjuje zaradi opravljanja naloge, ki je v javnem interesu (npr. državna statistika, raziskave po zakonu o raziskovalni dejavnosti, ipd.).

Več o pravici do ugovora:

→ Spletna stran tiodlocas.si: [Želim ugovarjati obdelavi mojih podatkov](https://tiodlocas.si/zelim-ugovarjati-obdelavi-mojih-podatkov)⁵³

na primer morala obstaja izrecna zakonska določba, posameznik pa bi se imel pravico seznaniti s tem, kakšna je smiselna logika odločanja (merila, pogoji, ponderji itd.).

Več o pravicah in postopku uveljavljanja pravic:

→ Smernice IP [Vodnik po varstvu osebnih podatkov za posameznike](https://www.ip-rs.si/publikacije/prirocnik-in-smernice-po-splo%27ni-uredbi-o-varstvu-podatkov-gdpr/vodnik-po-varstvu-osebni-podatkov-za-posameznike)⁵⁴



- **PRAVICA, DA ZA POSAMEZNIKA NE VELJA AVTOMATIZIRANA ODLOČITEV VKLJUČNO S PROFILIRANJEM (ČLEN 22);** Ta pravica posebej utrjuje posameznikov položaj, ko se o določenih pravnih ali za posameznika pomembnih zadevah odloča na podlagi avtomatiziranega (strojnega) odločanja z uporabo posameznikovih profilov. Ta pravica bi v šolstvu hipotetično prišla v poštev, če bi se na primer ocene dodeljevale na podlagi avtomatiziranega odločanja (npr. z uporabo vhodnih podatkov, računalnik pa bi po algoritmu vrnil oceno). Za zakonitost takšnega ocenjevanja bi

⁵³ <https://tiodlocas.si/zelim-ugovarjati-obdelavi-mojih-podatkov/>

⁵⁴ <https://www.ip-rs.si/publikacije/prirocnik-in-smernice-po-splo%27ni-uredbi-o-varstvu-podatkov-gdpr/vodnik-po-varstvu-osebni-podatkov-za-posameznike>

8 EVIDENCE DEJAVNOSTI OBDELAVE OSEBNIH PODATKOV

8.1 Zakaj je treba obdelave osebnih podatkov evidentirati?

Splošna uredba v členu 30 zahteva, da upravljavec in obdelovalec vodita 'evidenco dejavnosti obdelave osebnih podatkov'. Gre za sistematičen popis zbirke osebnih podatkov in postopkov, po katerih se obdeluje osebne podatke. Evidenca dejavnosti mora minimalno vsebovati taksativno predpisane informacije o obdelavi podatkov, kot so: kategorija podatkov, skupina posameznikov, na katere se osebni podatki nanašajo, namen obdelave, uporabniki podatkov itd. Na zahtevo nadzornega organa za varstvo osebnih podatkov morajo biti evidence dejavnosti v celoti na voljo.

Treba je opozoriti, da so nekatere »evidence«, predpisane tudi s področno zakonodajo, npr. na kadrovske področju z Zakonom o evidencah na področju dela. Pri tem pa je treba razlikovati med evidencami, ki vsebujejo osebne podatke (zbirke osebnih podatkov) in evidencami dejavnosti obdelav, ki zgolj kažejo na obstoj določene aktivnosti oziroma obdelave osebnih podatkov. Evidence dejavnosti obdelave osebnih podatkov, ki jih upravljavec ali obdelovalec vodi v skladu s členom 30 Splošne uredbe namreč niso zbirka osebnih podatkov, temveč so neke vrste indeks za mapiranje vseh zbirk in obdelav, ki jih izvaja organizacija na vseh področjih svojega delovanja. Lahko bi tudi rekli, da so **evidence dejavnosti obdelav kazalo za pregled po obdelavah osebnih podatkov, ki jih izvaja organizacija**. Zato so tudi pogosto v središču inšpekcijskih pregledov, saj služijo za izhodišče pri nadaljnji presoji skladnosti obdelave osebnih podatkov.

Z evidentiranjem dejavnosti obdelav osebnih podatkov se omogoča pregled nad zbirkami osebnih podatkov in obdelavami, ki jih šola izvaja z avtomatiziranimi sredstvi. Evidentiranje je način izkazovanja skladnosti, hkrati pa pomaga šoli, da bolje pozna svoje procese in zato tudi lažje odreagira na zahteve posameznikov in nadzornega organa, ko pride do vprašanj varstva osebnih podatkov.

8.2 Za koga velja obveznost evidentiranja?

Obveznost ustvarjanja evidenc o dejavnostih obdelave ni naložena le upravljavcu in njegovemu predstavniku, temveč tudi neposredno obdelovalcu in njihovim predstavnikom, kot je določeno v členu 30(2) Splošne uredbe. To je novost, ki jo v zvezi z evidentiranjem dejavnosti obdelave osebnih podatkov dodaja Splošna uredba in je posledica poudarjenega načela odgovornosti. Takšna zahteva gre z roko v roki z dejstvom, da je obdelovalec po Splošni uredbi v vlogi »pomočnika« upravljavca pri zagotavljanju skladnosti. To pa pomeni tudi, da imata tako upravljavec kot obdelovalec dolžnost voditi evidenco za isto dejavnost obdelave osebnih podatkov. Splošna uredba namreč ne vsebuje določbe, ki bi odvzemala odgovornost enega ali drugega, če kateri koli že vodi evidenco glede konkretne obdelave, zato bi morali pri pripravi evidenc upravljavci in obdelovalci delovati usklajeno in v sodelovanju.

8.3 Kdaj je evidentiranje obvezno in kdaj ne?

Izjema od splošne obveznosti evidentiranja vseh obdelav osebnih podatkov velja le za organizacije z manj kot 250 zaposlenimi IN če *obdelava verjetno ne bo ogrozila pravic in svoboščin posameznika*, na katerega se nanašajo osebni podatki, in če *ne gre za obdelavo posebne vrste osebnih podatkov ali osebne podatke v zvezi s kazenskimi obsodbami in prekrški* in če *se obdelavo opravi le občasno* (člen 30 (5) GDPR). **V praksi izjema od splošne obveznosti evidentiranja za manjše upravljavce ali obdelovalce, z manj kot 250 zaposlenimi, redko pride v poštev.** Težave se pojavijo zlasti pri razlagi tega, katera obdelava se šteje za »občasno«, saj se v večini organizacij - tudi ob široki razlagi izraza - podatke običajno redno obdeluje, na primer: obdelava podatkov na spletni strani (piškotki in druge sledilne tehnologije), sistemi za izračun plač zaposlenih, vodenje sistema za upravljanje odnosa s strankami (ang. CRM). Težava nastopi tudi pri razlagi – kdaj obdelava »verjetno predstavlja tveganje za pravice in svoboščine posameznikov«, na katere se nanašajo osebni podatki. Zlasti v zvezi s tem zadnjim kriterijem, velja opozoriti, da šola obdeluje osebne podatke otrok, čigar položaj je po Splošni uredbi bolj varovan. Šola pa kot institucija javnega sektorja izvršuje tudi javne naloge in je zato v razmerju do učencev v nadrejenem položaju.

Podobno tudi v razmerju do svojih zaposlenih. V obeh primerih je *tveganje za pravice in svoboščine posameznikov večje* in je zato v skladu s pravili Splošne uredbe, da šole obdelave osebnih podatkov, ki jih izvajajo, ustrezno evidentirajo.

8.4 Kaj morajo vsebovati evidence dejavnosti obdelave?

V evidence dejavnosti obdelave morajo **UPRAVLJAVCI** vključiti vse informacije, ki so navedene v členu 30(1) Splošne uredbe, in sicer:

- (a) naziv ali ime in **kontaktne podatke** upravljavca in, kadar obstajajo, **skupnega upravljavca**, predstavnika upravljavca in pooblaščenega osebe za varstvo podatkov;
- (b) **namene** obdelave;
- (c) opis **kategorij posameznikov**, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;
- (d) **kategorije uporabnikov**, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah (v to sodijo tudi obdelovalci)
- (e) kadar je ustrezno, **informacije o prenosih** osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z navedbo te tretje države ali mednarodne organizacije, v primeru prenosov iz drugega pododstavka člena 49(1) pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- (f) kadar je mogoče, predvidene **roke za izbris** različnih vrst podatkov;
- (g) kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov** iz člena 32(1).

Poleg navedenih informacij je priporočljivo, da **upravljavci** v evidence vključijo **tudi naslednje informacije**:

1. *naziv zbirke/dejavnosti obdelave*; kjer se opredeli za kakšno obdelavo/postopek/dejavnost gre.
2. *pravno podlago*; pravno podlago je nujno izkazati za zakonito obdelavo osebnih podatkov in ker so evidence v prvi vrsti namenjene

izkazovanju skladnosti je ustrezno, da vsebujejo tudi pravno podlago za evidentirano obdelavo.

3. *odgovorna oseba za posamezno dejavnost/zbirko*; ta oseba ni pooblaščenega oseba za varstvo osebnih podatkov, temveč je običajno oseba, ki izvaja dejavnost pri kateri pride do obdelave osebnih podatkov ali neposredno nadzira izvajanje te dejavnosti obdelave. Smisel navedbe odgovorne osebe je, da se v zvezi s posamezno dejavnostjo najlažje pride do relevantnih informacij prek osebe, ki relevantne informacije v zvezi z obdelavo ima.
4. *rezultat in sklic na oceno učinkov*, če je bila izvedena; Ko obstaja *visoko tveganje* za pravice in svoboščine posameznikov je obvezno izvesti oceno učinkov na varstvo osebnih podatkov. Zlasti pri uporabi (spletnih) IT rešitev v šolstvu, kjer se obdeluje osebne podatke otrok in se jih tudi prenaša v tretje države, obstaja povečana nevarnost visokega tveganja za pravice in svoboščine posameznikov in je lahko posledično obvezno izvesti oceno učinkov pred pričetkom izvajanja obdelave osebnih podatkov (npr. pred pričetkom uporabe nove aplikacije za izvajanje pouka na daljavo).

➔ Na voljo je **VZOREC: Vzorec evidence dejavnosti obdelave za UPRAVLJAVCE (člen 30 Splošne uredbe)**⁵⁵

V evidence dejavnosti obdelave morajo **OBDELOVALCI** vključiti vse informacije, ki so navedene v členu 30(2) Splošne uredbe, in sicer:

- (a) naziv ali ime in **kontaktne podatke** obdelovalca ali obdelovalcev in **vsakega upravljavca**, v imenu katerega deluje obdelovalec, **ter, kadar obstajajo, predstavnika upravljavca ali obdelovalca**, in **pooblaščenega osebe za varstvo podatkov**;
- (b) **vrste obdelave**, ki se izvaja v imenu posameznega upravljavca;
- (c) kadar je ustrezno, **prenose** osebnih podatkov v tretjo državo ali mednarodno organizacijo,

⁵⁵ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/OBRAZEC_-_Evidenca_dejavnosti_obdelave_osebnih_podatkov_ZA_UPRAVLJAVCE.docx

vključno z navedbo te tretje države ali mednarodne organizacije, v primeru prenosov iz drugega pododstavka člena 49(1) pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;

(d) kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov** iz člena 32(1).

8.5 PRIMERI

Izvajanje pouka na daljavo prek video-konferenčnega programa. V tem primeru se obdelujejo osebni podatki učencev in učiteljev. Učenci in učitelji so v podrejenem položaju v razmerju do šole, obdelavi se ne morejo izogniti, zato ta obdelava osebnih podatkov verjetno predstavlja tveganje za pravice in svoboščine posameznikov. Glede na navedeno je skladno s kriteriji iz člena 30(5) Splošne uredbe, to obdelavo **obvezno evidentirati**. Opredele se na primer:

- **naziv dejavnosti obdelave:** video-konferenca za izvajanje pouka z uporabo platforme Zoom;
- **kontaktni podatki upravljavca in pooblaščen osebe:** Osnovna šola..., naslov; pooblaščen oseba za varstvo osebnih podatkov: Ime Priimek, zaposlena na šoli;
- **namen in pravna podlaga:** osebne podatke učencev se obdeluje na podlagi člena 6(1)(e) Splošne uredbe, ker je obdelava potrebna za izvajanje naloge v javnem interesu, ki jo izvaja upravljavec in sicer za namen izvajanja programa osnovnošolskega izobraževanja v skladu z Zakonom o osnovni šoli; osebne podatke učiteljic in učiteljev na podlagi 48. člena Zakona o delovnih razmerjih, ker je to potrebno za izvajanje njihovih obveznosti iz delovnega razmerja
- **kategorije posameznikov:** učenci Osnovne šole, učitelji Osnovne šole;
- **kategorije uporabnikov:** Pogodbeni obdelovalec Zoom Video Communications, Inc.; učiteljski zbor;
- **informacija o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo:** osebne podatke se prenaša v ZDA in druge

države, kjer ima pogodbeni obdelovalec vzpostavljeno svojo infrastrukturo v skladu s pogodbo z obdelovalcem in na podlagi sprejetih standardnih pogodbenih klavzul, ki jih je sprejela Evropska Komisija.

- **rok za izbris:** osebni podatki se ne hrani, brišejo se sprotno ob poteku komunikacije/posamezni deli poka se snemajo in se hranijo največ do konca tekočega šolskega leta.
- **opis tehničnih in organizacijskih varnostnih ukrepov:** dostop do vsakokratne seje (npr. učne ure) je omejen zgolj za povabljenе udeležence (npr. učence in učitelja posameznega razreda); uporablja se dvofaktorska identifikacija; prenos je šifriran od vira do ponora (end-to-end AES-256 GCM meeting encryption);
- **Odgovorna oseba za obdelavo:** učitelj/učiteljica za izvajanje videokonference v svojem razredu.

Več o evidencah dejavnosti obdelave osebnih podatkov:

➔ Spletna stran IP: [Evidenca dejavnosti obdelave](#)⁵⁶

⁵⁶ <https://www.ip-rs.si/?id=105>

9 OCENA UČINKOV NA VARSTVO OSEBNIH PODATKOV

Ocena učinkov je orodje za pravočasno identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki. **Kadar je možno, da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, morajo upravljavci pred obdelavo, izvesti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov.** Ocena učinkov se lahko nanaša in izvede za posamezen proces obdelav osebnih podatkov ali pa za več procesov (podobnih) obdelav osebnih podatkov. IP je sprejel tudi obvezujoče kriterije, ki določajo v katerih primerih je ocena učinkov obvezna. [Seznam obdelav, kdaj je ocena učinkov obvezna se nahaja tukaj](#).⁵⁷

Kot je bilo že večkrat omenjeno, se obdelava osebnih podatkov otrok in zaposlenih šteje za obdelavo z višjim tveganjem, zlasti zaradi nesorazmerja moči med upravljavcem in posameznikom. Posebno tveganje predstavlja tudi uporaba novih tehnologij, kot tudi možnost prenosa osebnih podatkov v tretje države. Vse navedeno je treba upoštevati pri oceni, ali je za konkretno predvideno obdelavo obvezno izvesti oceno učinkov.

Treba je poudariti, da ko je v šolstvu vpeljava IT rešitev namenjena za podporo vodenju zakonskih zbirk, kjer se praviloma **obdelujejo tudi posebne vrste osebni podatki** (gibalne sposobnosti in morfološke značilnosti učencev, podatki v zbirki za pomoč oziroma svetovanje, kot so družinske, socialne, razvojne anamneze) in glede na **velik obseg obdelovanih osebnih podatkov ranljive skupine otrok – takšna obdelava osebnih podatkov predstavlja veliko tveganje, za pravice in svoboščine posameznikov in je zato predhodna ocena učinkov obvezna.** Zato IP v nadzornih postopkih tudi zahteva od upravljavcev, da izkažejo izvedeno oceno učinkov.

⁵⁷ https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejani_obdelav_osebni_podatkov_za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebni_podatkov.pdf

Smisel izvedbe ocene učinkov je predhodna ocenitev tvegane obdelave, da se preveri, s katerimi ukrepi je mogoče zmanjšati raven tveganja na takšno, da je obdelavo še dopustno izvajati. Če je po sprejetih ukrepih tveganje ublaženo na sprejemljivo raven, potem je obdelava dopustna, ocena učinkov pa kaže na to, da upravljavec pred obdelavo sistematično ocenil tveganje in sprejel potrebne ukrepe za zagotovitev skladnosti obdelave osebnih podatkov. Če je ocenjena raven tveganj tudi po sprejetih ukrepih še visoka, potem se mora upravljavec posvetovati z IP, v skladu s členom 36 Splošne uredbe. Vsakokrat, ko upravljavec izvaja oceno učinkov, pa mora za mnenje glede tvegane obdelave povprašati tudi pooblaščen osebo za varstvo osebnih podatkov.

Ali bi bilo treba za posamezne obdelave osebnih podatkov v šolstvu predhodno izvesti oceno učinkov na varstvo osebnih podatkov pa je treba ugotovljati v konkretnem primeru, upošteva kriterije, izpostavljene v kontrolnem seznamu. Treba pa je poudariti, da bo glede na vrsto visoko tveganih dejavnikov pri obdelavi osebnih podatkov v šolstvu (velik obseg podatkov, osebni podatki otrok, zaposlenih, posebne vrste osebnih podatkov) izvedba predhodne ocene učinkov pogosto obvezna.

Več o tem, kaj mora vsebovati ocena učinkov in kdaj jo je obvezno izvesti najdete na:

- ➔ Pojasnilo na spletni strani IP: [Ocena učinka v zvezi z varstvom podatkov](#)⁵⁸
- ➔ Smernice IP: [Smernice ocene učinkov na varstvo osebnih podatkov](#)⁵⁹

⁵⁸ <https://www.ip-rs.si/?id=101>

⁵⁹ <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-ocene-u%C4%8Dnikov-na-varstvo-osebni-podatkov> .

10 KRŠITEV VARNOSTI OSEBNIH PODATKOV

10.1 Kaj je kršitev varnosti?

Kršitev varnosti osebnih podatkov Splošna uredba ureja v členih 33 in 34 in pomeni kršitev, ki vodi do nenamerne ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja oziroma dostopa do osebnih podatkov. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Kršitve varnosti osebnih podatkov so v praksi lahko npr.:

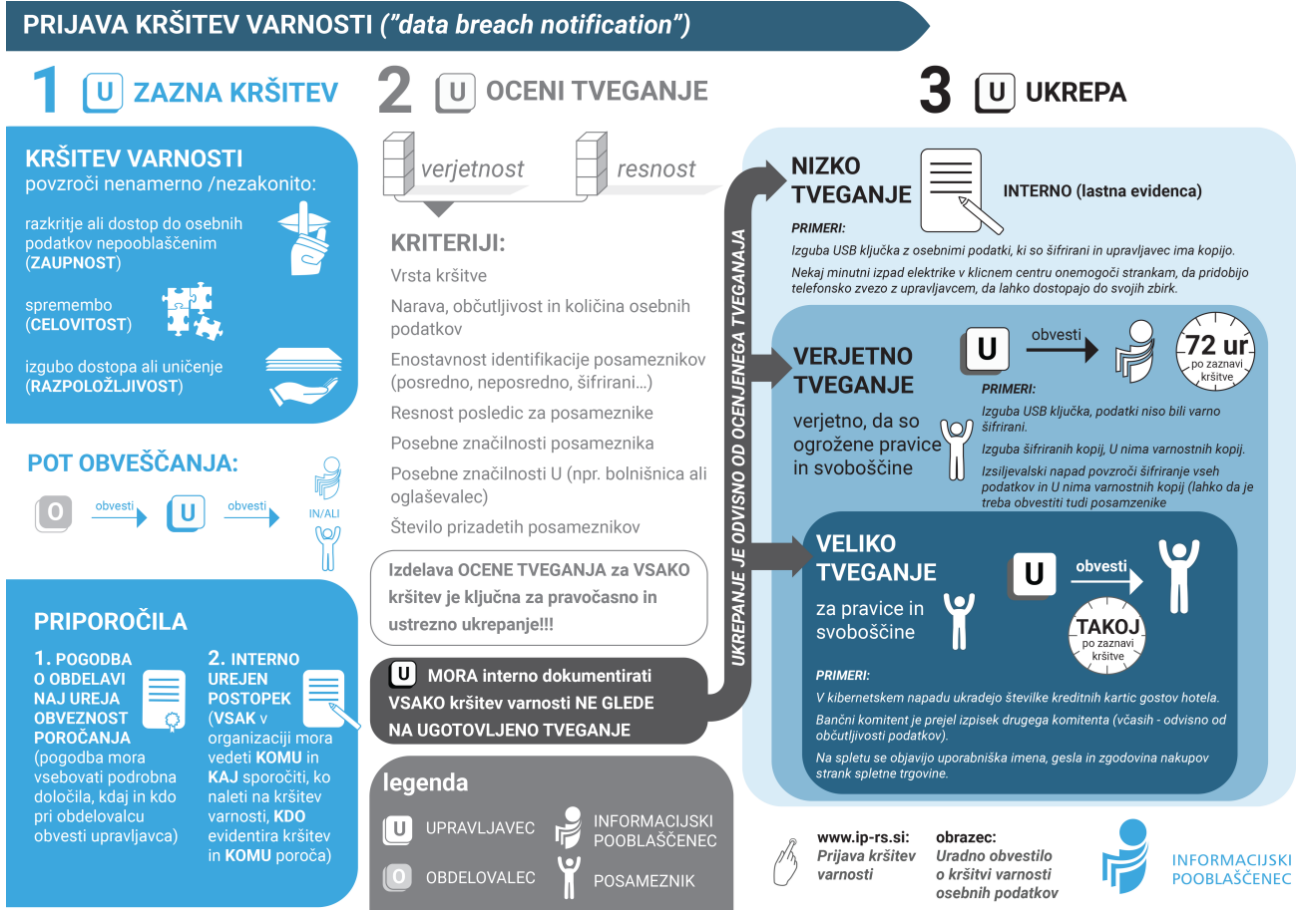
- dostop do osebnih podatkov s strani nepooblaščenih oseb;
- posredovanje osebnih podatkov nepravemu naslovniku;
- izguba ali kraja računalniške opreme, na kateri se nahajajo osebni podatki;
- nepooblaščen uničenje zbirk z osebnimi podatki;

Ko upravljavec zazna kršitev varnosti, mora oceniti tveganje, in kadar obstaja verjetno tveganje za pravice in svoboščine posameznikov, mora o kršitvi obvestiti IP (člen 33 Splošne uredbe). Če je tveganje veliko, mora o kršitvi varnosti obvestiti tudi posameznike (člen 34 Splošne uredbe).

- sprememba osebnih podatkov brez potrebnega dovoljenja;
- izguba dostopa do osebnih podatkov (izguba gesla; izguba opreme, ki omogoča dešifriranje; nepooblaščen namestitev šifrirnega programa, ki onemogoča dostop do podatkov, t.i. »izsiljevalski virus«).

10.2 Kako mora ukrepati upravljavec, če zazna kršitev varnosti?

Postopek za ravnanje upravljavca, ko zazna kršitev varnosti je IP opredelil tudi v infografiki:



Kršitev varnosti se lahko sporoči IP na neobveznem obrazcu ([neobvezen obrazec za podajo obvestila o kršitvi](#))⁶⁰, Splošna uredba pa predpisuje minimalno vsebino, ki jo mora vsako obvestilo vsebovati.

10.3 Kakšni sta vloga in odgovornost obdelovalcev?

Obdelovalci so dolžni obvestiti upravljavca **o vsaki kršitvi varnosti takoj, ko kršitev zaznajo**. Ta obveznost mora biti zapisana tudi v pogodbi o obdelavi osebnih podatkov. Obdelovalec mora upravljavcu zagotoviti vse potrebne informacije za oceno tveganj posledic kršitve. Od te ocene bo odvisno, ali mora upravljavec podati uradno obvestilo o kršitvi IP.

Primer: Šola pri ponudniku informacijske storitve (obdelovalec), koristi storitve hrambe podatkov o učencih, komunikacije s starši ipd. Obdelovalec zazna vdor v svoj informacijski sistem in nepooblaščen dostop do baz podatkov, ki jih vodi za namene upravljavca. Obdelovalec incident nemudoma sporoči upravljavcu, ki nato o tem poda uradno obvestilo IP.

Več o tem:

- Spletna stran IP: [Prijava kršitev varnosti](#)⁶¹
- [Smernice s primeri prijav kršitve varnosti](#)⁶²

OBRAZEC:

- [Neobvezen obrazec za podajo obvestila o kršitvi](#)⁶³

⁶⁰ [https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/OBRAZEC - Obvestilo o krsitvi 18.3.2019.docx](https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/OBRAZEC_-_Obvestilo_o_krsitvi_18.3.2019.docx)

⁶¹ <https://www.ip-rs.si/?id=106>

⁶² https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en

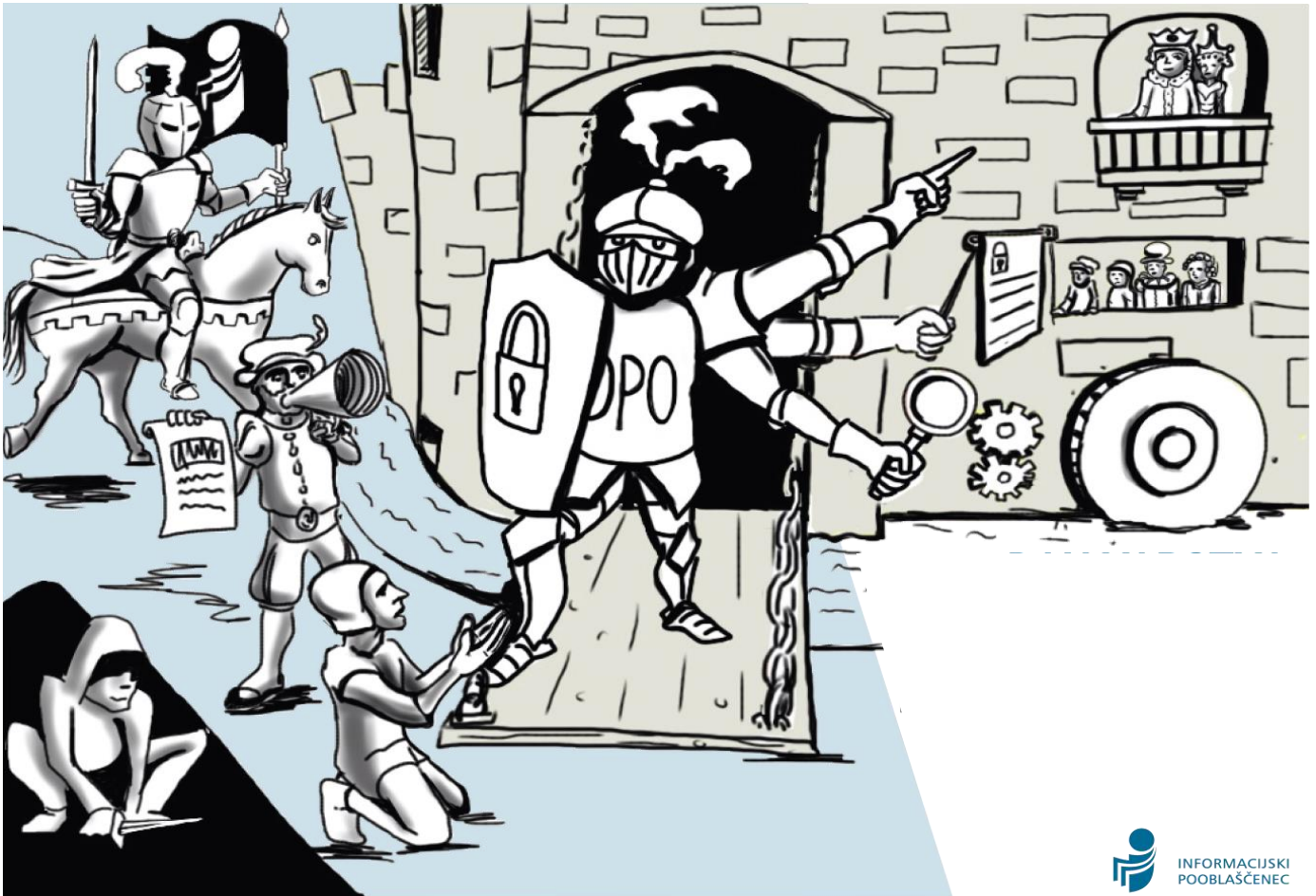
⁶³ [https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/OBRAZEC - Obvestilo o krsitvi 18.3.2019.docx](https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/OBRAZEC_-_Obvestilo_o_krsitvi_18.3.2019.docx)

11 VLOGA POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV

11.1 Kdo je pooblaščen oseba za varstvo osebnih podatkov?

Pooblaščen oseba za varstvo podatkov (ang. Data Protection Officer ali »DPO«), ki deluje pri upravljavcu (ali za upravljavca) izvaja svetovalne in nadzorne naloge na področju varstva osebnih podatkov. Šole so kot druge organizacije iz javnega sektorja po večini vestno pristopile k zagotavljanju pooblaščen osebe za varstvo osebnih podatkov. Pomembno je, da ima pooblaščen oseba, ki deluje pri organizaciji v skladu s členom 39 Splošne uredbe, več nalog, in sicer:

- (a) **obveščanje** upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter **svetovanje** navedenim o njihovih obveznostih v skladu s to uredbo in drugimi določbami prava Unije ali prava države članice o varstvu podatkov;
- (b) **spremljanje skladnosti** s to uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
- (c) **svetovanje**, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s členom 35;
- (d) **sodelovanje z nadzornim organom**;
- (e) delovanje kot **kontaktna točka** za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz člena 36, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.



11.2 Kako lahko pomaga pooblaščen oseb za varstvo osebnih podatkov?

IP prepozna vlogo pooblaščen oseb za varstvo osebnih podatkov kot ključno za zagotavljanje skladnosti, zlasti v okoliščinah, ko se je treba prilagoditi na spremenjene družbene in zdravstvene razmere. Kot je bilo opisano v teh smernicah, so tveganja pri uporabi IT rešitev resna in jih je treba skladno z zakonodajo nasloviti pred pričetkom izvajanja obdelave. Mnoge obdelave so povezane s sklepanjem ustreznih pogodb, zagotavljanem pogojev za prenose v tretje države, evidentiranjem, zagotavljanjem informacij itd. Vse te obveznosti imajo svoj smisel in cilj, da se zaščitijo, v konkretnem primeru pravice in svoboščine otrok in zaposlenih v šolstvu. Za izpolnjevanje teh obveznosti pa je treba zagotoviti strokovno usposobljen kader, ki bo znal z nasveti, usmeritvami in pojasnili usmerjati izvajanje obdelav osebnih podatkov v skladu z zakonodajo. **Prav institut pooblaščen oseb za varstvo osebnih podatkov pa je namenjen temu, da se zagotovi nujno potrebna podpora za izpolnjevanje obveznosti zakonodaje.**

Pooblaščen oseb za varstvo osebnih podatkov bi morale biti prve, ki bi ob posvetovanju s svojimi sodelavci s področja informacijskih tehnologij svetovale v zvezi s pripravo **ocene učinkov na varstvo osebnih podatkov pri uporabi** posamezne IT rešitve in spremljale **izvajanje tvegane obdelave**. Za izpolnitev obveznosti privzetega in vgrajenega varstva osebnih podatkov, bi pooblaščen oseb morale tvorno sodelovati v vseh fazah obdelave – od izbire IT rešitve, do spremljanja njihovega izvajanja. Pomembno pa je, da se pooblaščen oseb pravočasno vključi v postopek določanja sredstev obdelave osebnih podatkov, saj se lahko le tako zagotovi, da nudijo **ustrezno strokovno podpora**:

- (a) **vodstvu** (običajno ravnatelj, včasih tudi svetu zavoda ali staršev za nadstandardne storitve), za sprejem informiranih odločitev glede izbire ponudnikov in sklenitve ustreznih pogodb o obdelavi osebnih podatkov;
- (b) **administratorjem informacijske podpore**, da bi vgradili ustrezne nastavitve in informacije glede obdelav osebnih podatkov, ki **končnim**

uporabnikom zagotavljajo pravočasno in ustrezno informiranje ter varno in skladno uporabo IT rešitve.

Kljub temu, da Splošna uredba zahteva imenovanje pooblaščenih oseb, kadar je upravljavec ali obdelovalec javni organ ali telo – šole zaradi pomanjkanja sredstev pogosto ne imenujejo pooblaščenih oseb za varstvo osebnih podatkov ali pa jih imenujejo zgolj formalno, tako da imenovane osebe niso ustrezno strokovno usposobljene ali pa se jim ne zagotavlja pogojev za opravljanje vseh nalog, ki jih imajo kot pooblaščen oseb za varstvo osebnih podatkov. Po mnenju IP je nujno, da šole skupaj z drugimi deležniki, ki vplivajo na financiranje šol, zagotovijo potrebna sredstva tudi na tem področju – saj so pooblaščen oseb za varstvo osebnih podatkov tiste, ki lahko ključno prispevajo k zagotavljanju skladnosti organizacije na področju varstva osebnih podatkov. Splošna uredba omogoča tudi, da več javnih organov ali teles ob upoštevanju njihove organizacijske strukture in velikosti imenuje eno samo pooblaščen oseb za varstvo podatkov. Pooblaščen oseb pa tudi ni nujno zaposlena oseb pri šoli, temveč je lahko tudi zunanji izvajalec. IP je prepričan, da je slovenski izobraževalni sistem ob ustreznih organizacijski in finančni prilagoditvi sposoben zagotoviti potrebno znanje in izkušnje za zagotovitev skladnosti na področju varstva osebnih podatkov.

12 ZAKLJUČEK

Pričujoče smernice z mnogimi praktičnimi primeri osvetljujejo problematiko varstva osebnih podatkov pri uporabi IT storitev v šolstvu. Treba se je zavedati, da ko na primer učitelj izvaja videokonferenco ali ko prejema gradivo od učencev in na drug način, z njimi komunicira prek elektronskih sredstev (npr. prejema ali posreduje fotografije, videe, druge izdelke učencev) ali objavi oziroma omogoča dostop do teh vsebin z uporabo elektronskih sredstev, pri tem praviloma vedno pride do obdelave osebnih podatkov. Narava prenosov podatkov po elektronskih omrežjih pa je takšna, da se podatki prenašajo bliskovito hitro in po celem svetu, kar izpostavlja posameznike v komunikaciji različnim tveganjem (tako učence ali dijake, kot tudi učitelje). Zato Splošna uredba uvaja stroga pravila, ki zajemajo tako pogoje za samo obdelavo (katere podatke, za kakšen namen, na kateri pravni podlagi) in informiranje končnih uporabnikov, kot tudi pogoje za določitev sredstev obdelav, t.j. izbiro ponudnikov IT storitev in njihovih IT rešitev (na podlagi ocen učinkov ali tveganj za pravice in svoboščine, vgrajenega in privzetega varstva, varnosti obdelav itd.), pogoje za prenose v tretje države, itd. Za vse navedeno so odgovorni

upravljavci osebnih podatkov, to so šole in njihove odgovorne osebe, to so večinoma ravnatelji.

IP se zaveda, da je prva skrb vsake šole učinkovito izvajanje izobraževanja. Zato je nujno, da se šolam omogoči uporaba učinkovitih in varnih IT rešitev, ki zagotavljajo tudi skladnost s pravili varstva osebnih podatkov. Ker je izbira ponudnikov, kot tudi določanje pogojev uporabe IT storitev v šolstvu zelo tehnološko in pravno zahtevna, bi bilo absolutno nujno, da šole pri tem niso prepuščene same sebi (ali celo, da se izbira prepušča posameznemu učitelju), temveč da se k problemu pristopi enotno na ravni celotne države. Pri tem IP apelira zlasti na resorno ministrstvo, da sestavi delovno skupino, ki bo preučila možnosti za učinkovite in varne IT rešitve ter izdala ustrezne usmeritve, katere IT rešitve in kako naj jih uporabljajo šole in učitelji. Pričujoče smernice pa so pri tem lahko v pomoč za zagotavljanje skladnosti na področju varstva osebnih podatkov.





Priloga: kontrolni seznami za skladnost

I. Zakonitost obdelave pri izbrani informacijski rešitvi

➤ OPREDELITEV NAMENA

- (a) Katero IT rešitev uporabljate (aplikacija, program, itd.)? Navedite ime programa/aplikacije in če ista aplikacija omogoča več storitev, tudi posamezne storitve.

Npr.

- Arnes učilnice, Arnes Video, Arnes Videokonference, Zoom, Google Drive, Dropbox itd.

- (b) Čigavi osebni podatki se obdelujejo? Opredelite **kategorije posameznikov**.

Npr.

- Učitelji/ice, drugi zaposleni
- Učenci/dijaki
- Starši/zakoniti zastopniki

- (c) Zakaj uporabljate posamezno IT rešitev? **Opredelite namen oz. namene uporabe** te IT rešitve.

Npr.

- Arnes videokonference se uporablja za poučevanja/predavanja in pisno/ustno ocenjevanje; za izvajanje govornih ur, roditeljskih sestankov; za kolegije, sestanke zaposlenih itd.;
- Dropbox za shranjevanje izdelkov učencev, za izobraževanje in ocenjevanje;
- ...

➤ OPREDELITEV PRAVNE PODLAGE

- (a) Ali imate zagotovljeno pravno podlago za obdelavo za vsak opredeljen namen? **Pri vsakem specifičnem namenu** pripišite **pravno podlago**, po kateri se obdeluje osebne podatke.

Npr.

- Za izvajanje pouka in ocenjevanja po Arnes videokonferenci – je nujno za izvajanje naloge v javnem interesu (člen 6(1)(e) Splošne uredbe, v zvezi s četrtem odstavkom 9. člena ZVOP-1 v zvezi z ustreznim členom področne zakonodaje, ki določa, da je izvajanje pouka in izobraževanje javno-pravna naloga šole);
- Za objavo na spletu z namenom promocije šole – privolitev (člen 6(1)(a) Splošne uredbe);
- Za izvajanje sestankov med zaposlenimi – 48. člen Zakona o delovnih razmerjih;
- ...

- (b) Če je podlaga **privolitev** posameznika (učenca/dijaka starejšega od 18 let ali starša ali skrbnika), najprej preverite, ali je privolitev v konkretnem primeru sploh dopustna, ali je ustrezno zagotovljena možnost izbire in ali so/bodo spoštovani preklici privolitve? Navedite, **kako je zagotovljena prostovoljnost privolitve.**

Npr.

- Privolitev se upošteva pri objavi dosežkov učencev na spletni strani šole (npr. tekmovanja). Privolitev za ta namen je pridobljena od staršev v začetku šolskega leta. Če starši ne podajo privolitve, se dosežka učenca ne objavi.
- Privolitev se pridobiva, ko to zahteva zakon (npr. ZOsn v 95. členu določa, da se podatki v zbirko podatkov o gibalnih sposobnostih in morfoloških značilnostih učencev, zbirajo na podlagi soglasja staršev ali skrbnika).

➤ STRUKTURIRANJE NAMENOV

Za pomoč pri evidentiranju namenov in pravne podlage predlagamo, da informacije strukturirate po naslednjem modelu:

IT REŠITEV	NAMEN IN PRAVNA PODLAGA	KATEGORIJE POSAMEZNIKOV
Arnes videokonferenca	Izvajanje pouka; člen 6(1)(e) GDPR, v zvezi z ... (člen področne zakonodaje)	Učenci/učitelji
	sestanki s starši; člen 6(1)(e) GDPR, v zvezi z ... (člen področne zakonodaje)	Starši/učitelji
	sestanki z zaposlenimi; 48. člen ZDR-1	zaposleni
Arnes Video	Objava na splet (javno) – za promocijo; člen 6(1)(a) GDPR (privolitev)	Učenci/učitelji
	Objava v učilnico (interno) – za izvajanje pouka; člen 6(1)(e) GDPR, v zvezi z ... (člen področne zakonodaje)	Učenci/učitelji

II. Varnost in odgovornost pri izbrani informacijski rešitvi

➤ ZAGOTAVLJANJE SPOŠTOVANJA NAČEL

- (a) Ali se podatki uporabljajo izključno za namen, za katerega so bili podatki zbrani – ali se uporabljajo še za kak drug (dodatni) namen? Opredelite za vsak namen posebej. (zagotavljanje načela **omejitve namena**).

PRIMER: Za izvajanje pouka in ocenjevanje se izdelki učencev (pisni izdelki, fotografije, itd.) shranjujejo v oblaku, kamor učenci odlagajo svoje prispevke v mape. Ti osebni podatki se uporabljajo izključno za ta namen. Za morebiten drug namen – npr. objava osebnih podatkov

učenca na spletu za promocijo šole, se izvede v soglasju s starši oziroma skrbniki (za mlajše od 15 let) oziroma učencem/dijakom samim (če je dopolnil 15 let)..

- (b) Ali je obdelava sorazmerna glede na opredeljen namen? Premislite za vsak namen obdelave posebej, ali so osebni podatki *ustrezni, relevantni in omejeni na to, kar je potrebno* za namene, za katere se obdelujejo (zagotavljanje načela **najmanjšega obsega podatkov**).

PRIMER: Učitelj zahteva uporabo le tistih aplikacij in orodij, ter na način, ki ga predvidi šola. Učitelj ne zahteva uporabe aplikacij, ki se namestijo na zasebne telefone, ki bi zbirale tudi dodatne osebne podatke, ki niso potrebni za izvajanje izobraževanja (npr. za merjenje telesnih aktivnosti, lokacije ipd.).

- (c) Ali se podatki shranjujejo **le minimalno potreben čas**? Premislite za vsak namen posebej, ali ima šola sprejete ukrepe, ki preprečujejo hrambo podatkov dlje, kot je potrebno za namen zbiranja (načelo **omejitve hrambe**); Obdobje hrambe za posamezen namen obdelave se sporoča tudi v *informacijah posameznikom* (člena 13 in 14 Splošne uredbe, poglavje 7 pričujočih smernic) in interno vodi v *evidencah dejavnosti obdelave* (člen 30 Splošne uredbe, poglavje 8 pričujočih smernic)

PRIMER: Učitelj zahteva, da učenci naložijo fotografije/posnetke/pisne izdelke itd. opravljenih aktivnosti v skupno mapo. Podatki se hranijo le do konca šolskega leta, potem se podatki brišejo. Treba je preveriti, ali so vsi učitelji seznanjeni z določenimi roki hrambe za posamezen namen obdelave, ali so roki ustrezno evidentirani v evidencah dejavnosti obdelave in ali so posamezniki o rokih tudi ustrezno informirani (ali so informacije za posameznike ustrezno posodobljene glede na namen hrambe).

- (d) Kako je **zavarovan prenos** podatkov? Opredelite za vsako IT rešitev posebej.

PRIMER: Program, ki omogoča videokonference zagotavlja kriptiran prenos podatkov po elektronskem omrežju od vira do ponora.

- (e) Kako je zagotovljena **varnost za hrambo** zbirk osebnih podatkov?

PRIMER: Program/aplikacija, ki omogoča oblačno hrambo, v skladu s pogodbo o obdelavi s ponudnikom in izbranimi nastavitvami, zagotavlja hrambo podatkov v kriptirani obliki.

➤ **SPREJETA INTERNA PRAVILA IN POLITIKE**

- (a) Ali je šola sprejela in opredelila **ukrepe za skladno obdelavo osebnih podatkov** (npr. interni pravilnik, navodilo itd.)?

Po ZVOP-1 so morali vsi upravljavci iz javnega sektorja (tudi šole) sprejeti »Pravilnik o zavarovanju osebnih podatkov«, v katerem so morali biti predpisani tehnični in organizacijski ukrepi za varno obdelavo osebnih podatkov. Splošna uredba sicer izrecno ne zahteva, da

upravljavci sprejemajo »Pravilnik o zavarovanju«, zahteva pa, da upravljavci sprejmejo ustrezne ukrepe za zagotavljanje skladne obdelave osebnih podatkov, sprejem teh ukrepov pa morajo biti sposobni tudi izkazati (člena 24 in 25 Splošne uredbe). **Po vsebini se torej še vedno zahteva sprejem internih pravil za ravnanje z osebnimi podatki, ki pa morajo pokrivati vsa področja skladnosti – tako varnost (celovitost, razpoložljivost in zaupnost), kot tudi spoštovanje drugih načel, kot je najmanjši obseg podatkov, omejitev namena in omejitev shranjevanja, itd. Dodatne obveznosti po Splošni uredbi so tudi vodenje evidence dejavnost obdelave in ocena učinkov na varstvo osebnih podatkov (več o tem glej poglavje 8 in 9 predmetnih smernic).**

- (b) Ali interni pravilnik ureja tudi pogoje za obdelavo osebnih podatkov pri uporabi informacijskih storitev?

Pravila za skladno obdelavo osebnih podatkov bi morala vključevati navodila za ravnanje učiteljev in drugih zaposlenih na šoli v zvezi z uporabo IT rešitev, s katerimi se obdeluje osebne podatke. Interna pravila/navodila za skladno obdelavo osebnih podatkov bi morala vključevati:

- Opredelitev, **katero** IT rešitve se uporablja na šoli (npr. katero videokonferenco, rešitev za nalaganje in predvajanje video/foto vsebin itd.);
- Opredelitev IT rešitev bi morala biti **razdelana glede na namen** (npr. izvajanje pouka, sestankovanje zaposlenih, promocija šole itd.) **in dalje glede na funkcionalnost** (npr. shranjevanje posnetkov, fotografij, izdelkov, izvajanje konferenčnega video klica, objava podatkov na spletu itd.);
- Za vsako IT orodje bi morala obstajati enotna **navodila za nastavitev uporabe** – tako, da se zagotavlja »privzeto« varstvo osebnih podatkov (člen 25 Splošne uredbe);
- Za shranjene podatke bi morali biti predvideni **roki hrambe**.

Če interna pravila/navodila tega ne opredeljujejo, potem je treba obvestiti vodstvo šole in pooblaščen osebo za varstvo osebnih podatkov, da se pristopi k njihovi ustrezni dopolnitvi.

- (c) Ali so bili ukrepi **posodobljeni** glede na pogoje **šolanja na daljavo**? Ali so bile posodobljene **evidence dejavnosti obdelave**? Ali je bila izvedena ocena učinkov v zvezi z novimi obdelavami osebnih podatkov?

Šolanje na daljavo je zlasti z uporabo IT rešitev pomembno povečalo tveganje za neskladno obdelavo osebnih podatkov. Nujno bi bilo, da bi bila ustrezno naslovljena tudi tveganja v zvezi s tem. To se zagotavlja s preverjanjem novih obdelav osebnih podatkov – tako, da se obdelave najprej ustrezno opredeli v evidencah dejavnosti obdelave, po potrebi izvede ocene učinkov in v nadaljevanju sprejme ustrezne ukrepe in navodila za izvajanje konkretne obdelave osebnih podatkov.

PRIMER: Pred pričetkom izvajanja pouka na daljavo šola izbere ustrezno videokonferenčno rešitev, preveri, ali ima dejavnost obdelave ustrezno evidentirano in po potrebi izvede oceno učinkov (zlasti na primer, če učitelji IT rešitev uporabljajo tudi pri ocenjevanju znanja). Po izvedeni oceni učinkov sprejme pravilnik, v katerem opredeli, kako naj se IT rešitev uporablja, da se bo zagotovilo izpolnjevanje vseh načel varstva osebnih podatkov.

III. Pogodbena obdelava pri izbrani informacijski rešitvi

- (a) Ali izbrani ponudnik informacijske rešitve nudi storitev obdelave osebnih podatkov? Pojasnite, kako ponudnik informacijske rešitve obdeluje osebne podatke (kako deluje kot obdelovalec).

Pojasnilo: Treba je vedeti, ali z uporabo določene aplikacije/storitve (1.) pride do obdelave osebnih podatkov in (2.) ali to obdelavo izvaja tretja oseba oziroma ponudnik storitve.

PRIMER 1: Učiteljica izvaja pouk na daljavo prek videokonference. Da pride do prenosa podatkov in da komunikacija deluje, mora obstajati zunanji izvajalec, ki zagotavlja storitev prek svojih strežnikov. Z izvajalcem storitve mora šola skleniti ustrezno pogodbo o obdelavi osebnih podatkov.

PRIMER 2: Učitelj zahteva od učencev, da mu posredujejo svoje prispevke / domače naloge po elektronski pošti, ki jih shrani na šolski računalnik v mape, ustvarjene na njihova imena. Pri tem pride do več avtomatiziranih obdelav osebnih podatkov. Pri prenosu se podatki shranijo pri ponudniku storitve elektronske pošte, s katerim mora šola imeti sklenjeno ustrezno pogodbo o obdelavi osebnih podatkov. Dalje, učitelj iz svojega predala elektronskih sporočil prenese datoteko in podatke shrani na računalnik v ustrezno mapo posameznega učenca. Hramba zbirke map učencev na šolskem računalniku je obdelava osebnih podatkov, ki se izvaja na strojni opremi šole in za to šola ne potrebuje zunanje storitve. Za namen hrambe osebnih podatkov šola nastopa kot samostojni upravljavec osebnih podatkov.

- (b) Ali ima šola z izbranim obdelovalcem sklenjeno **pisno pogodbo o obdelavi** osebnih podatkov?

Pojasnilo: Pogodba o obdelavi osebnih podatkov mora biti **vedno sklenjena v pisni obliki**. Preverite, ali imate za vsako storitev obdelave osebnih podatkov, ki vam jo zagotavlja zunanji izvajalec, sklenjeno ustrezno pogodbo o obdelavi osebnih podatkov.

- (c) Ali pisna pogodba vsebuje **vse elemente** iz člena 28 Splošne uredbe?

Pojasnilo: Pisna pogodba o obdelavi mora imeti vse bistvene elemente v skladu s členom 28 (3) Splošne uredbe. Na voljo so standardna pogodbeno določila, ki jih lahko uporabijo upravljavci kot vzorec za sklenitev ustrezne pogodbe o obdelavi osebnih podatkov (Standardna pogodbeno določila so dostopna so na tej [povezavi](#)⁶⁴).

- (d) S katerimi **tehničnimi in organizacijski ukrepi obdelovalec** skrbi za varno obdelavo osebnih podatkov?

Pojasnilo: Upravljavec mora sprejeti ustrezne tehnične in organizacijske ukrepe, ki zagotavljajo varno obdelavo osebnih podatkov (člen 32 Splošne uredbe). Slednje velja tudi, če upravljavec najame obdelovalca, zato mora upravljavec pogoje ustrezno opredeliti v pisni pogodbi o obdelavi osebnih podatkov. Opredelitev ustreznih tehničnih in organizacijskih ukrepov v pogodbi o

⁶⁴ https://www.ip-rs.si/fileadmin/user_upload/doc/Standardna_pogodbena_dolocila_-_clen_28_15jul2020.docx

obdelavi osebnih podatkov je torej obveznost upravljavca, saj prek tega izkazuje, da je zagotovil pogodbeno varovala za ustrezen nivo varne obdelave osebnih podatkov.

- (e) Ali pogodbeni obdelovalec za zagotavljanje svoje storitve najema »podizvajalce« (pod-obdelovalce)? Ali pogodba vključuje **izrecno ali splošno dovoljenje** za uporabo storitev »pod-obdelovalca«?

Pojasnilo: Po Splošni uredbi obdelovalec ne sme zaposliti drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca. V primeru splošnega pisnega dovoljenja, obdelovalec upravljavca obvesti o vseh nameravanih spremembah glede zaposlitve dodatnih obdelovalcev ali njihove zamenjave, s čimer se upravljavcu omogoči, da nasprotuje tem spremembam (člen 28(2) Splošne uredbe). Navedeno pomeni, da mora imeti upravljavec nadzor nad tem, koliko in katerega podizvajalca najame obdelovalec za obdelavo osebnih podatkov, za katere je odgovoren upravljavec.

- (f) Ali ste preverili, če bo obdelovalec (in ali podobdelovalec) morebitni prenašal osebne podatke v tretje države?

Pojasnilo: Upravljavec je dolžan v pisni pogodbi opredeliti tudi, ali bo obdelovalec prenašal osebne podatke v tretjo državo ali mednarodno organizacijo. To je obvezna sestavina pogodbe, hkrati pa mora upravljavec nedvomno vedeti in imeti nadzor nad tem, v katere države se bo osebne podatke prenašalo in pod katerimi pogoji. Podatke o prenosih mora upravljavec zagotavljati tako v informacijah posameznikom (člen 13(1)(f) in 14(1)(f) Splošne uredbe), kot tudi v evidencah dejavnosti obdelave osebnih podatkov.

PRIMER: Ponudnik oblachne hrambe (npr. Google Drive omogoča hrambo osebnih podatkov na strežnikih v ZDA). Šola mora preveriti, ali so izpolnjeni pogoji za tak prenos (več v nadaljevanju).

IV. Prenos osebnih podatkov v tretje države pri izbrani informacijski rešitvi

- (a) Ali se podatki pri uporabi izbrane informacijske rešitve **prenašajo v tretje države?**

Preveriti je treba zlasti, ali se z uporabo izbrane informacijske storitve osebni podatki prenašajo izven meja EGP (države članice EU in Norveška, Islandija, Lihtenštajn) – npr. strežnik, ki omogoča storitev, je v ZDA.

- (b) Če se prenašajo, ali za prenos **obstaja ustrezna (dodatna)** pravna podlaga?

Preveriti je treba, ali so zagotovljeni pogoji za zakonit prenos – npr. da se podatke prenaša v državo ali ozemlja, za katera velja, da zagotavljajo ustrezno raven varstva skladno s sklepom o ustreznosti Evropske Komisije; da so med šolo in ponudnikom sklenjene ustrezne standardne pogodbene klavzule ([Uradni list EU L 199 dne 7. junija 2021](#)) ipd.

V. Informiranje in zagotavljanje pravic v zvezi z izbrano informacijsko rešitvijo

➤ INFORMIRANJE

- (a) Ali so o obdelavi njihovih osebnih podatkov s konkretno informacijsko rešitvijo obveščeni učitelji/uslužbenci na šoli? Opredelite s katerimi sredstvi poteka informiranje (npr. interno izobraževanje zaposlenih, interna obvestila po elektronski pošti, interna navodila/akti/informacije itd.)

***Pojasnilo:** Ko na primer učitelj izvaja pouk po videokonferenci, se pri tem obdelujejo tudi osebni podatki učitelja. Šola, ki nastopa kot upravljavec osebnih podatkov, mora o obdelavi osebnih podatkov učitelja ustrezno informirati, z vsemi informacijami, ki jih predpisujeta člena 13 in 14 Splošne uredbe. To lahko na primer stori z obveščanjem po običajni poti (npr. elektronska pošta, pisno obveščanje na šoli itd.). Šola je kot upravljavec odgovorna, da izkaže, da so bile zaposlenim posredovane razumljive in ustrezne informacije glede obdelave njihovih osebnih podatkov.*

- (b) Ali so o obdelavi osebnih podatkov učencev/dijakov s konkretno IT rešitvijo seznanjeni posamezniki oz. zakoniti zastopniki (npr. starši/učenci/dijaki)? Opredelite s katerimi sredstvi poteka informiranje.

***Pojasnilo:** Enake vrste informacij, kot jih mora šola kot upravljavec posredovati učiteljem in zaposlenim, mora posredovati tudi učencem oziroma njihovih staršem/skrbnikom. Informacije se posredujejo na primeren način (npr. pojasnila pred izvajanjem pouka, na govorilnih urah, pisna obvestila po elektronski/navadni pošti itd).*

- (c) Ali je obvestilo prilagojeno za naslovnika, da lahko ta jasno razume zakaj (za kakšen namen) in kateri njegovi osebni podatki se obdelujejo s konkretno informacijsko rešitvijo ter kakšne so njegove pravice v zvezi s to obdelavo?

***Pojasnilo:** Skladno s Splošno uredbo morajo biti informacije jasne, razumljive in prilagojene, da jih razumejo naslovni posamezniki. Informacije morajo biti po potrebi razčlenjene in/ali večplastne. Informiranje mora biti izvedeno na način, ki je posamezniku dostopen, kar pomeni da morajo upravljavci posameznike informirati na običajen način.*

- (d) Ali obvestilo vsebuje vse informacije, ki jih zahtevata člena 13 oz. 14 Splošne uredbe?

Po vsebini mora obvestilo posameznikom vsebovati vse informacije, ki so taksativno naštet v členu 13 in 14 Splošne uredbe. Za informiranje lahko šola uporabi tudi pripravljen obrazec IP: [Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 13 Splošne uredbe\)](#),⁶⁵

⁶⁵ <https://www.ip->

[rs.si/fileadmin/user_upload/doc/vzorci/VZOREC_OBVESTILA_POSAMEZNIKOM_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx](https://www.ip-rs.si/fileadmin/user_upload/doc/vzorci/VZOREC_OBVESTILA_POSAMEZNIKOM_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx)

[Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 14 Splošne uredbe\).](#)⁶⁶

- (e) Ali je upravljavec (šola) sposobna vse zgoraj navedeno izkazati oziroma dokazati?

Pojasnilo: Upravljavec je odgovoren za ustrezno informiranje in mora biti to sposoben tudi izkazati ali dokazati na zahtevo nadzornega organa. Glede na navedeno je priporočljivo, da šola posredovane informacije ali navodila, kako naj se izvaja informiranje, hrani zato, da jih lahko posreduje na zahtevo nadzornega organa.

➤ PRAVICE POSAMEZNIKOV

- (a) Ali šola obravnava vse prejete zahteve za obravnavo pravic posameznikov?

Pojasnilo: Šole so kot upravljavci osebnih podatkov dolžne obravnavati zahteve posameznikov, ki uveljavljajo svoje pravice. Ker z uporabo IT rešitev nastajajo zbirke osebnih podatkov, lahko v zvezi s tem posamezniki (učenci/starši/skrbniki, učitelji kot zaposleni itd.) ravno tako uveljavljajo vse prej omenjene pravice po Splošni uredbi. Treba je poudariti, da posamezniki niso dolžni izrecno opredeliti pravne podlage za odločanje. Če je iz smisla zahteve razvidno, katero pravico uveljavljajo, so se dolžne šole na takšno zahtevo ustrezno odzvati.

- (b) Ali ima šola opredeljene protokole za obravnavo zahtev posameznikov v zvezi z njihovimi pravicami?

Pojasnilo: Šola je kot upravljavec osebnih podatkov dolžna obravnavati zahteve posameznikov v predpisanem roku enega meseca oziroma najkasneje v dveh dodatnih mesecih, če rok za odločanje podaljša v skladu s členom 12(3) Splošne uredbe. Nespoštovanje predvidenih rokov je kršitev Splošne uredbe in lahko zaradi tega upravljavec trpi tudi predpisane sankcije. Jasno mora biti opredeljeno, kdo obravnava prejete zahteve.

- (c) Ali je v zvezi z obravnavo zahtev posameznikov šola organizirala izobraževanje za zadevne zaposlene, ki rešujejo vloge posameznikov?

Pojasnilo: Šole kot upravljavci osebnih podatkov morajo imeti potrebno znanje in kadrovska podpro za obravnavo zahtev posameznikov. Zato je pomembno, da šole zagotovijo ustrezna izobraževanja za zaposlene, ki bodo obravnavali zahteve posameznikov.

⁶⁶ https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/OBVESTILO_POSAMEZNIKOM_PO_14_CLENU_SPLOSNE_UREDBE_O_VARSTVU_PODATKO_V_GDPR_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx

VI. Evidentiranje dejavnosti obdelav z izbrano informacijsko rešitvijo

- (a) Ali je mogoče vsako obdelavo osebnih podatkov, ki se izvaja z izbrano IT rešitvijo (ki je bilo opredeljeno uvodoma), uvrstiti v ustrezno evidenco in katero? Ali šola vodi ustrezne evidence tudi za tiste obdelave osebnih podatkov, ki jih izvaja pogodbeni obdelovalec in za katere mora ta voditi evidence v skladu s členom 30(2) Splošne uredbe?

Pojasnilo: Posamezno dejavnost obdelave osebnih podatkov, ki jo izvaja šola (tudi če jo zagotavlja s pomočjo zunanjega izvajalca), je treba umestiti v ustrezno evidenco dejavnosti obdelave. Pogosto že same pogodbe o obdelavi osebnih podatkov vsebujejo tudi evidence dejavnosti obdelave. Treba pa je preveriti v konkretnem primeru, ali so vse obdelave osebnih podatkov, ki se izvajajo (pregled po namenih in IT rešitvah), tudi ustrezno evidentirane.

- (b) Ali so v vsaki evidenci navedene vse zahtevane kategorije po 30(1) Splošne uredbe (vključno s podatki glede prenosov v tretje države)?

Pojasnilo: Informacije v evidencah ne smejo biti same sebi namen. Evidence bi morale biti živa dokumentacija, ki se jo po potrebi pregleduje in osvežuje. Zato bi morala pooblaščenca oseba za varstvo osebnih podatkov sprotno pregledovati evidence in opozarjati na morebitne pomanjkljivosti in predlagati ukrepe za zapolnitev morebitnih vrzeli.

VII. Ocena učinkov na varstvo osebnih podatkov

- (a) Ali boste z uporabo izbrane informacijske rešitve izvajali karkoli od naslednjega:
- ocenjevanje ali točkovanje;
 - avtomatizirano odločanje s pomembnimi učinki;
 - sistematično spremljanje;
 - obdelava občutljivih osebnih podatkov (posebnih vrst) ali podatkov zelo osebne narave;
 - obdelava v velikem obsegu;
 - obdelava podatkov o ranljivih posameznikih (ali posameznikih v podrejenem položaju), na katere se nanašajo osebni podatki;
 - inovativne tehnološke ali organizacijske rešitve;
 - uporabljali video in/ali avdio snemanje in/ali spremljanje;
 - obdelava, ki preprečuje posameznikom ali omejuje dostop do pravice / storitve / pogodbe;

- od vpeljave nove informacijske rešitve je minilo več kot 3 leta, spremenila pa se je narava, obseg, kontekst ali namen obdelave osebnih podatkov?

Če ugotovite, da boste z obdelavo izvedli karkoli od zgoraj naštetega, se glede tega, ali bo obvezno izvesti oceno učinka, pogovorite s pooblaščen osebo za varstvo osebnih podatkov.

- (b) Ali ste dokumentirali svoje razloge, če ste se odločili, da ocene učinkov ne boste izvedli?

***Pojasnilo:** Če se upravljavec odloči, da ocene učinkov ne bo izvedel, ker obdelava ne dosega praga visokega tveganja, potem mora skladno s evropskimi smernicami v zvezi z oceno učinkov na varstvo osebnih podatkov dokumentirati razloge, zakaj ocene učinka ni izvedel.⁶⁷*

VIII. Kršitev varnosti pri uporabi izbrane informacijske rešitve

Ali se je zgodilo karkoli od naslednjega, kar je ali bi lahko ogrozilo varnost osebnih podatkov?

- izgubljena ali ukradena naprava;
- izgubljen, ukraden ali na ne-varnem mestu puščen dokument;
- izgubljena ali odprta pošta;
- zlonamern vdor v informacijski sistem;
- zlonamerna programska oprema (npr. izsiljevalski virusi);
- lažno predstavljanje (t.i. »*phishing*«);
- nepravilno uničenje osebnih podatkov v fizični obliki;
- osebni podatki še vedno prisotni na zastareli napravi;
- nenamerna objava osebnih podatkov;
- osebni podatki, poslani napačnemu prejemniku;
- nepooblaščen verbalno razkritje osebnih podatkov;
- druga vrsta kršitve, ki bi lahko ogrozila *zaupnost, razpoložljivost* ali *celovitost* osebnih podatkov, ki jih obdeluje upravljavec.

Če ste zaznali, da se je zgodil varnostni incident, se nemudoma posvetujte s svojo pooblaščen osebo za varstvo osebnih podatkov in pristopite k ustreznemu ukrepanju.

⁶⁷ Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, DS 248 rev.01, <https://ec.europa.eu/newsroom/article29/items/611236>.