

Vodič po varstvu osebnih podatkov za starše in učitelje



INFORMACIJSKI
POOBLAŠČENEC



REPUBLIKA SLOVENIJA



INFORMACIJSKI
POOBLAŠČENEC

**Vošnjakova 1
1000 Ljubljana
gp.ip@ip-rs.si**

Projekt je finančno podprl predsednik Republike Slovenije.

Urednica: Nataša Pirc Musar
Avtorji: Klemen Mišič, Nataša Pirc Musar
Grafično oblikovanje: Klemen Mišič
Fotografije: *Fotolia*
Naklada: 110.000 izvodov

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

342.738(497.4)

MIŠIČ, Klemen
Samo ti odločaš: komu lahko zaupam osebne podatke in kdaj? / [avtorja Klemen Mišič, Nataša Pirc Musar]. - Ljubljana: Informacijski pooblaščenec, 2007

Vsebuje tudi besedilo, tiskano v obratni smeri: Vodič po varstvu osebnih podatkov za starše in učitelje

www.ip-rs.si

ISBN 978-961-91762-4-5
1. Pirc Musar, Nataša 2. Mišič, Klemen: Vodič po varstvu osebnih podatkov za starše in učitelje
236076032

Zakaj varovati osebne podatke?

Ocene in bolezni učencev, podatki o starših, videonadzor. To je le nekaj konkretnih primerov, v katerih ste kot učitelji zavezani spoštovati Zakon o varstvu osebnih podatkov (ZVOP-1). Informacijski pooblaščenec je v praksi vse pre-pogosto naletel na primere, ko šole tega področja niso poznale. Morda si ob branju tega besedila mislite, da In-formacijski pooblaščenec "spet" malo pretirava, ko poudar-ja pomen varstva osebnih podatkov. Odgovorjam z nekaj primeri, ki so delno izmišljeni, delno povzeti iz prakse:

- Roditeljski sestanek: Učitelj odpre redovalnico in starši otrok pogledajo vanjo. Pri tem učitelj pozabi prekriti ocene drugih in starši lahko vidijo tudi ocene od drugih učencev. Prihodnji dan eden od otrok doživi zasmehovanje, saj so drugi starši prek svojih otrok prenesli svoje negativne poglede na določenega učenca.

- Pri vходу v šolo je nameščena kamera, ki snema širši prostor in dvorišče. Posnetki so shranjeni na računalniku, ki ni zaščiten z geslom. Radovedni učitelj, ki ima sina na tej šoli in kateremu je nekdo namignil, da sin "šprica" določene ure, "vdre" v računalnik in ugotovi, da se njegov sin skrivaj dobiva z mnogo starejšim dekletom, ki ga z avtomobilom na določene dneve čaka pred šolo. Ali je učitelj ravnal prav? Ali pa drug primer: Sosed prosi učitelja, naj mu pove domači naslov učiteljice, ki mu je všeč.

- Učenec zboli za občutljivo in nenavadno boleznijo. Učitelj vrsto bolezni med poukom razkrije drugim učencem ali komu od staršev. Bolnega učenca po vrnitvi v šolo sošolci izključijo ali zasmehujejo.

Za vas, starše, velja enako. Varovanje osebnih podatkov ni le vaša pravica in pravica vaših otrok, pač pa tudi vaša dolžnost, ko gre za osebne podatke (drugega) otroka ali starša.

Brošura, ki jo prebirate, je napisana tako, da lahko tako učenci kakor tudi starši in učitelji spoznate pravice in dolžnosti drugih udeležencev v procesu izobraževanja, ki se dotikajo temeljne človekove pravice do zasebnosti, ka-tere ožji del je pravica do varstva osebnih podatkov. Če boste poznali osnove, boste brez dvoma lahko lažje in učinkoviteje odpravili morebitne napake, ki se v vsakdanjem šolskem življenju lahko zgodijo - hote ali nehote. S tem ne boste samo koristili ugledu otrok, pač pa se boste izognili tudi prekrškovnemu postopku, odškodninskim tožbam in "tečnim" nadzornikom. Zato se zavedajmo pomena varstva osebnih podatkov in začnimo na začetku – pri varovanju.

Nataša Pirc Musar, univ. dipl. prav.
Informacijska pooblaščenka RS



"Porablajte denar za nakup zasebnosti, saj vam v življenju večino časa ni dovoljeno, da bi bili normalni."

Johnny Depp





Kaj je osebni podatek?

Zakon o varstvu osebnih podatkov (ZVOP-1) določa, da je osebni podatek katerikoli podatek, ki se nanaša na posameznika, pri čemer mora biti posameznik določena ali določljiva fizična oseba.

ZVOP-1 torej varuje samo tiste podatke, za katere vemo, kateri osebi pripadajo (oz. je ta oseba vsaj določljiva). Določenost oz. določljivost se presoja po različnih kriterijih, po najenostavnejšem se je treba samo vprašati, ali vemo, komu neki osebni podatek pripada. Določenost je torej treba presojati posebej, od primera do primera. Slovencem najbolj znan primer je določenost posameznika Janeza Novaka. Če temu imenu in priimku dodamo podatek o tem, da je Janez Novak Slovenec, posameznika prav gotovo ne moremo določiti, saj je v Sloveniji okrog 7700 posameznikov s takšnim imenom in priimkom. Če imenu in priimku dodamo, da ima Janez Novak prebivališče v Ljubljani, krog posameznikov sicer zožimo, vendar posameznik še vedno ni določljiv. Ko pa Janeza Novaka povežemo z njegovim domačim naslovom (ali npr. imenom majhne vasi), posameznik postane vsaj določljiv, če že ne določen. Takoj ko gre za določljivo osebo, osebni podatki, ki se nanašajo na to osebo, postanejo varovani osebni podatki v smislu ZVOP-1 (razen, če seveda kak zakon ne določa drugače). V takem primeru je njihova obdelava strožje urejena.

Seveda pri tem ne gre pozabiti, da ZVOP-1 varuje samo osebne podatke, ki so del zbirke ali so namenjeni vključitvi vanjo. Takšna ureditev sicer ne pomeni, da posamezniki, ki jim je nekdo posegel v njihovo pravico do zasebnosti, nimajo pravnega varstva, ampak le, da imajo drugačno obliko pravnega varstva (ne prek Informacijskega pooblaščenca, temveč prek sodišča v pravnem ali kazenskem postopku zaradi katerega od t. i. verbalnih deliktov).

Podatki o gospodarskih družbah, samostojnih podjetnikih posameznikih (v delu, ki se nanašajo na njihovo opravljanje dejavnosti), državnih organih ipd. torej niso osebni podatki in jih ZVOP-1 ne varuje.



Obdelava

Obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja z osebnimi podatki.

Definicija obdelave osebnih podatkov je torej izjemno široka. Zato je pomembno, da se ob vsakem ravnanju z osebnimi podatki zavedamo pravil in določil ZVOP-1, ki določajo, kdaj in pod kakšnimi pogoji lahko osebne podatke obdelujemo. V nasprotnem primeru lahko hitro posežemo v zasebnost posameznika (pravica do varstva osebnih podatkov je del širše ustavne pravice do zasebnosti), lahko pa se tudi hitro znajdemo v prekrškovnem postopku (ZVOP-1 določa kazni 4170 eurov za pravno osebo in 830 eurov za odgovorno osebo pravne osebe) ali, celo hujše, tvegamo odškodninsko tožbo in celo kazenski pregon (ob hujših zlorabah osebnih podatkov).

Obdelava osebnih podatkov v javnem sektorju

Javni sektor lahko osebne podatke obdeluje samo, če je obdelava osebnih podatkov določena v zakonu, na podlagi osebne privolitve pa znova, če je takšna obdelava določena v zakonu.

Šole torej ne smejo obdelovati osebnih podatkov, če jim tega ne dopušča zakon. Izjema, ki jo pozitivna zakonodaja dopušča, velja v primerih, kadar šola neke dejavnosti ne izvaja v okviru svojega "oblastnega" (torej v okviru javnega pooblastila) delovanja, torej izvajanja tistih dejavnosti, ki ji jih predpisuje zakon. V takih primerih veljajo glede obdelave osebnih podatkov pravila zasebnega sektorja. Pomembno pa je poudariti, da šola "oblastnega" delovanja ne sme kategorizirati v "neoblastno" delovanje.

Primer izjeme: neformalni piknik staršev in učiteljev, šola želi fotografije objaviti na svoji spletni strani. Ker neformalno srečanje ne sodi v okvir oblastnega delovanja šole, ta fotografije lahko objavi zgolj na podlagi osebne privolitve staršev.

Druga izjema pa določa, da se lahko v javnem sektorju (v katerega sodijo tudi vzgojno-izobraževalne ustanove) izjemoma 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. Izjemo je treba razumeti ozko.

Tak primer je dolžnost vrtcev in šol, da centrom za socialno delo (CSD) na lastno pobudo ali na njihovo zahtevo posredujejo določene osebne podatke v primeru suma zlorabe otroka. Zakon o socialnem varstvu namreč izrecno določa, da so organi ter zavodi in druge organizacije, ki pri svojem delu ugotovijo ogroženost otroka, mladoletnika ali osebe, ki ji je vzeta poslovna sposobnost, o tem dolžni obvestiti CSD na svojem območju. K prijavi dolžnosti vrtce in šole zavezuje tudi kazenski zakonik. Hkrati so vrtci in šole ter druge organizacije javnega sektorja CSD-ju na njegovo zahtevo dolžni posredovati osebne podatke iz svojih zbirk, ki se nanašajo na (domnevno) ogrožene otroke za potrebe izvedbe ukrepov po posebnih predpisih. Takšna obdelava osebnih podatkov in s tem njihovo posredovanje sta dopustna in zakonita. Pri tem je CSD upravičen le do tistih osebnih podatkov, ki so resnično potrebni in primerni za odločitve o primernih ukrepih in za izvedbo le-teh, kar je treba presojati v vsakem konkretnem primeru posebej. Po naravi stvari pa lahko dejansko le CSD oceni, kateri podatki utegnejo biti zanj pomembni. Zato je CSD zavezan k odgovornemu pristopu pri podajanju zahtev za posredovanje osebnih podatkov – vsaka pisna zahteva mora biti v zadostni meri obrazložena, šole in vrtci pa kot upravljalci CSD-ju ne smejo posredovati več podatkov, kot je potrebno.





Svetovni splet in elektronska pošta

Elektronska pošta

Pri elektronski pošti je pomembno najprej razmejiti službeno elektronsko pošto in zasebno pošto, ki ni povezana s službeno (npr. pošta prek strežnikov Gmail, Hotmail ...).

Dejstvo je, da je zasebna pošta vedno zasebna in je nihče ni upravičen pregledovati (razen s sodnim nalogom organi pregona). To pomeni, da niti starši niti učitelji ne smejo pregledovati zasebne pošte otrok, saj je tajnost pisma (kamor sodi tudi zasebnost elektronske pošte) ustavno zagotovljena pravica tako otrok kot tudi zaposlenih v šoli.

Glede pregledovanja službene elektronske pošte (med katero se lahko vrine tudi kako zasebno sporočilo) pa je treba najprej omeniti sodbo Evropskega sodišča za človekove pravice v zadevi *Copland v. Velika Britanija* (*Application no. 62617/00*, sodba z dne 3. 4. 2007). V tem primeru je sodišče delavki priznalo širok krog pravice do zasebnosti in presodilo, da je delodajalec neupravičeno posegal v njeno zasebnost. Ključni element sodbe je bil prav ta, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira e-pošto.

Če torej delodajalec službeno pošto zaposlenega želi pregledovati, mora zaposlenemu pravila za takšen ukrep sporočiti vnaprej, ali v obliki pravilnika ali v obliki drugega ustreznega akta, ki ga izda ravnatelj. Če tega ne bo storil, lahko močno poseže v zasebnost zaposlenega in tvega posledice.

Učenci načeloma ne uporabljajo "šolske" pošte. Če jo, morajo biti ravno tako vnaprej opozorjeni, kakšno pošto lahko pošiljajo in kdaj lahko šola vpogleda v e-pošto. Nikakor pa šola ne sme pregledati zasebne e-pošte učencev, čeprav ti pošto pošiljajo s šolskega računalnika. Zasebna je tudi komunikacija med učiteljem in staršem.

Najpogostejša zloraba osebnega podatka staršev, ki so šoli dali svoj e-naslov, je napačno pošiljanje e-obvestil vsem staršem. Šole namreč pozabijo uporabiti t. i. BCC rubriko, ki omogoča preprečiti razkritje e-poštnega naslova vsem naslovnikom. Če namreč pošiljatelj e-naslave vnese v rubriko To ali CC, vsi starši pridobijo in vidijo e-naslave vseh ostalih staršev, kar je neupravičeno razkrivanje osebnih podatkov. Ne pozabite, tovrstne adreme so zelo mamljive za pošiljanje raznih reklam (neposredno trženje), kar mnogi starši, nezavedajoč se zakonske prepovedi takšnega ravnanja, storijo, ali še huje, kak starš, ki ima rad e-šale, začne tudi vsem ostalim pošiljati »e-neumnosti«, kar je nadlegovanje nekoga, ki želi imeti svoj e-naslov samo za komuniciranje s šolo, ne pa tudi za komunikacijo z ostalimi starši.

Uporaba svetovnega spleta

Kako in kdaj lahko učenci in zaposleni v šoli uporabljajo splet, je določeno s pravili, ki jih določi šola. Vprašanje seveda je, kdo lahko nadzira pravilnost uporabe spleta. Osnovno pravilo je, da nihče nima pravice vedeti, kdo je obiskoval kako spletno stran, saj s tem ugotovimo vsebino ogleda. Dopustno je slediti, katere strani so najpogostejše obiskane, a zgolj v anonimizirani obliki – torej tako, da informatik ali druga odgovorna oseba ugotovi, katere spletne strani obiskujejo zaposleni in učenci, ne da bi bilo pri tem mogoče ugotoviti, kdo je obiskal točno določeno spletno stran.

Ob upoštevanju zgoraj opisane sodbe Evropskega sodišča za človekove pravice v primeru *Copland v. Velika Britanija* je najčistejša rešitev, da šola vnaprej onemogoči obiskovanje spletnih strani z določeno vsebino (npr. s filtri) oziroma omogoči samo ogled tistih spletnih strani, ki so potrebne za izobraževanje otrok.

Primer člena, ki definira pravico do vpogleda v e-pošto:

Oseba, zadolžena za delovanje računalniškega informacijskega sistema, lahko na posebej utemeljeno pisno zahtevo ravnatelja v prisotnosti komisije opravi nadzor in pregled elektronske pošte zaradi uvedbe ali vodenja sodnega, prekrškovnega, disciplinskega ali drugega postopka, povezanega z delovnim razmerjem. V izrednih primerih (nenadna odpoved delavca ali drug izreden dogodek) lahko ravnatelj ali za to pooblaščen oseba vpogleda v elektronsko pošto le, če je to nujno potrebno za vodenje delovnega procesa.

Da bi bili učenci in zaposleni ustrezno seznanjeni s tem, kaj lahko na spletu ali z e-pošto počnejo in česa ne, mora šola vnaprej izdelati jasna pravila in z njimi seznaniti otroke in zaposlene. Pri tem jih je treba opozoriti na morebitne sankcije, če pravil ne bodo spoštovali.

Pravila so lahko neoblična in jih lahko šola prilagodi glede na svoje potrebe. Šolam je lahko v pomoč vzorec pravilnika o zavarovanju osebnih podatkov, ki je objavljen na spletni strani pooblaščenca:



Načelo sorazmernosti

Načelo sorazmernosti določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.

To načelo je najpomembnejše načelo na področju varstva osebnih podatkov in je nekakšen korektor za vse tiste primere, ki jih določa ZVOP-1 ali kak drug zakon, ki ureja obdelavo osebnih podatkov, pa jih ne našteje taksativno.

Tudi v šolah bodite pozorni, da od učencev in staršev zbirate samo tiste osebne podatke, ki jih resnično potrebujete za doseg namena, za katerega jih zbirate in nato obdelujete.





Zavarovanje

ZVOP-1 določa, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki.

Verjetno gre za najpomembnejša določila zakona, ki posamezniku omogočajo, da zaupa v varnost svojih osebnih podatkov, ki jih zaupa upravljavcu. Zakon določa, da mora upravljavec osebne podatke zaščititi tako, da je onemogočeno celo njihovo naključno uničenje ali zloraba. Gre za zahtevno nalogo, ki jo zakon nalaga upravljavcem osebnih podatkov, a treba se je zavedati, da je zloraba osebnih podatkov hud poseg v zasebnost posameznika in je zato treba osebne podatke resnično dobro varovati.

Posebej poudarjamo, da bodite pozorni na obstoj t. i. sledljivosti obdelave osebnih podatkov, saj se pri tem v praksi dogaja največ kršitev – tudi v šolah. Sledljivost pomeni, da morate kot upravljavec osebnih podatkov za vsako obdelavo (torej tudi za vpogled) omogočiti poznejše ugotavljanje, kdaj so bili osebni podatki v zbirko osebnih podatkov vneseni (torej zbrani), posredovani ali obdelani in kdo je to storil. Predvsem pa je naloga ravnatelja, da natančno opredeli, kdo od zaposlenih ima pravico do vpogleda v določene zbirke osebnih podatkov.

Podrobnejše so ti postopki zavarovanja, kakor tudi zavarovanje informacijskih sistemov, opisani v brošuri Informacijskega pooblaščenca z naslovom *Zavarujmo osebne podatke, priročnik za upravljavce* – najdete jo na spletni strani v pdf obliki na naslovu <http://www.ip-rs.si/publikacije/prirocniki/>.



Kako torej zaščititi?

Informacijski pooblaščenec se je v svoji praksi že nekajkrat srečal s težavami glede obdelave osebnih podatkov v šolstvu. V nadaljevanju predstavljamo nekaj najpogostejših kršitev in odgovarjamo na nekaj najpogostejših vprašanj, ki jih je prejel od staršev, učiteljev, pa tudi učencev.

Prikazani primeri naj služijo vam, spoštovani učitelji in starši, da boste lažje prepoznali kršitve ZVOP-1 in se boste nanje ustrezno odzvali. Naj vam pomagajo pri vsakdanjem delu, tako da do kršitev sploh ne bi prišlo.

Vpogled v redovalnico

Ena najpogostejših kršitev. Učitelji pokažejo redovalnico staršem, pri tem pa ne zakrijejo podatkov (ocen) drugih učencev. Tako staršem omogočijo tudi vpogled v ocene drugih otrok.

Rešitev so posebni prekrivniki, ki omogočajo samo vpogled v ocene izbranega otroka. Najenostavneje pa je z dvema listoma papirja prekriti vse ostale osebne podatke otrok. Enako velja za roditeljske sestanke – osebnih podatkov otrok ne razkrivajte drugim staršem. Rekli boste, da otroci doma sami povedo za ocene drugih. Zagotovo ne vsi in zagotovo ne za vse otroke. Šola kot upravljavalec te pravice nima in se mora tega držati.

Objave fotografij in videoposnetkov

Objava fotografij in videoposnetkov na spletni strani šole je dovoljena samo

takrat, kadar starši v to privolijo in če taka objava osebnih podatkov sodi v okvir neoblastnega delovanja šole (npr. družabna srečanja, dogodki ...).

Poudarjamo, da privolitve učencev ni pravno veljavna do 18. leta (v nekaterih primerih do 15. leta, torej do pridobitve poslovne sposobnosti), in še enkrat opozarjamo, da morate za privolitev vprašati starše, ki so otrokovi zakoniti zastopniki. Enako velja tudi za obdelavo vseh tistih osebnih podatkov, za katerih obdelavo ne obstaja zakonska podlaga (npr. zborniki učencev).

Objave različnih seznamov otrok na oglasnih deskah

Z objavo seznamov se vedno razkrijejo osebni podatki otrok, in to ne le drugim otrokom in njihovim staršem, pač pa tudi vsem obiskovalcem, ki vstopijo v šolo.

Zato Pooblaščenec priporoča, da šole seznamov ne objavljajo na vidnih mestih (na primer na vhodnih vratih šole, kjer je ta seznam dostopen vsem mimoidočim), pač pa naj poiščejo tak način obveščanja, ki ne bo posegal v zasebnost otrok.

Anketiranje učencev

Šola, ki želi anketirati učence, lahko to izvede brez privolitve staršev, če so ankete anonimne in so vprašanja zastavljena tako, da se iz morebitnih odgovorov ne da izluščiti, kateri učenec je na anketo odgovarjal (izjeme so seveda z zakonom predpisane ankete). V ostalih primerih boste morali v šolah zaprositi za dovoljenje staršev.

Zdravstveni podatki o učencih

Nedopustno je, da otrokom ali drugim učiteljem razkrijete bolezen ali poškodbo, zaradi katere je učenec odsoten. Podatki o zdravstvenem stanju so namreč občutljivi osebni podatki in šola jih nima pravice zbirati in obdelovati. To pomeni, da šola pri starših otrok (niti pri otrocih samih) ne sme poizvedovati po diagnozi, pač pa lahko pridobi samo obvestilo zdravnika oz. starša, da je otrok odsoten zaradi bolezni. Prav tako šola nima pravice poizvedovati o zdravstvenem stanju pri drugih institucijah ali posameznikih. Izjema je sum na nalezljive bolezni, pri katerih lahko šola obvesti pristojnega zdravnika in starše ter o pojavu primera nalezljive bolezni tudi Inštitut za varovanje zdravja, pri čemer je zdravnik odgovoren za ukrepanje naprej. Šola oziroma vrtec pa v okviru splošnih ukrepov za preprečevanje in obvladovanje nalezljivih bolezni le obvesti inštitut o pojavu, ne sme pa mu posredovati osebnih podatkov. Starši se seveda lahko sami odločijo, kdaj bodo učitelju povedali kaj več.

Vpogled staršev v osebni karton njihovega otroka

Staršu otroka ne smete odreči vpogleda v osebni karton, redovalnico ipd., tudi če sta starša ločena in eden od staršev šoli prepove vpogled za drugega starša. Takšna prepoved je irelevantna. Edina izjema je odvzem roditeljske pravice starša. Tak starš do otroka nima nobenih pravic in dolžnosti.



Videonadzor

Videonadzor v šolah je dovoljen le za varovanje vstopov v šolo in izstopov iz nje, varovanje svojega premoženja (npr. parkirišče pred šolo), samo v izjemnih primerih pa je dovoljen tudi videonadzor delovnih prostorov.

Pred uvedbo videonadzora mora šola o njegovi uvedbi pisno obvestiti vse zaposlene in učence. Prav tako mora namestiti obvestilo o izvajanju videonadzora, ki mora vsebovati naslednje informacije:

1. informacijo o tem, da se videonadzor izvaja;
2. naziv šole, ki ga izvaja;
3. telefonsko številko, na kateri lahko posameznik dobi informacije o videonadzoru.

Obvestilo je treba namestiti pred območje, kjer se videonadzor izvaja. Šola praviloma ne sme izvajati videonadzora razreda. Prav tako videonadzor ni dovoljen v garderobah, dvigalih in sanitarnih prostorih. Zakon namreč te prostore šteje za prostore zasebnosti.

Videonadzor delovnih prostorov je mogoč le v izjemnih primerih, kadar je to nujno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovnih skrivnosti, tega namena pa ni mogoče doseči z milejšimi sredstvi. Primeri, v katerih bo šola lahko izvajala videonadzor delovnih prostorov, bodo torej redki.

Če se vendarle izkaže, da obstaja potreba po videonadzoru delovnih mest, se mora šola pred uvedbo posvetovati z reprezentativnim sindikatom, pisno obvestiti zaposlene, ki bodo nadzorovani, in videonadzor omejiti le na tiste dele, kjer je ta nujno potreben. Praksa je pokazala, da zavezanci le redko upravičijo videonadzor delovnih prostorov, zato uvedbo takega načina nadzora odsvetujemo, če niste popolnoma prepričani, da izpolnujete pogoje.



Biometrija

Biometrija je izraz, ki ga ZVOP-1 uporablja za telesne, fiziološke ter vedenjske značilnosti, ki jih imajo vsi posamezniki, so pa edinstvene in stalne za vsakega posameznika posebej ter je z njimi posameznika mogoče določiti, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, dezoksiribonukleinske kisline (DNK) ter značilne drže.

Šola lahko biometrijo uvede samo, če je to nujno potrebno za:

- opravljanje dejavnosti;
- varnost ljudi ali premoženja;
- varovanje tajnih podatkov ali poslovnih skrivnosti.

Šola lahko biometrijske ukrepe izvaja le nad svojimi zaposlenimi, če so bili o tem predhodno pisno obveščeni (torej NE nad otroki). Treba je poudariti, da mora šola v primeru, v katerem ji uporabo biometrije ne določa zakon, pridobiti odločbo Informacijskega pooblaščenca. Pred prejemanjem pozitivne odločbe je uporaba biometrije prepovedana.

Informacijski pooblaščenec se je tudi v praksi že srečal z uporabo biometrije v šoli. Bila je neupravičena.

Pooblaščenec poudarja, da bo redko katera šola – če ji seveda drugače ne določa zakon – izkazala upravičenost uporabe biometrije. Zavedati se je namreč treba, da je v večini primerov varnost in nadzor mogoče zagotoviti z milejšimi sredstvi (npr. z videonadzorom), zato biometrijo v vsakem primeru uporabljajte izredno previdno, saj pomeni velik poseg v zasebnost posameznika.