



**DATU VALSTS INSPEKCIJA**

**Datu valsts inspekcijas  
rekomendācija  
Bērnu datu aizsardzība skolās**

Rīga, 2011.gads

## Ievads

Palielinoties informācijas apjomam, kas ir skolu rīcībā, kā arī pieaugot informācijas tehnoloģiju izmantošanai, aizvien vairāk uzmanība jāpievērš normatīvajiem aktiem personas datu aizsardzības jomā, un jo īpaši diviem aspektiem: fiziskas personas tiesības un pienākumi.

Fizisko personu datu aizsardzības likums nosaka principus kā vākt, apstrādāt, glabāt personas datus.

Saistībā ar iepriekš minēto šī rekomendācija ir sagatavota ar mērķi sniegt atbildes uz jautājumiem, kas attiecas uz bērnu personas datu aizsardzību skolās, īpaši respektējot bērnu tiesības attiecībā uz privātumu.

## Definīcijas

Fizisko personu datu aizsardzības likums (turpmāk- likums) attiecas uz visu veidu personas datu apstrādi un jebkuru fizisko vai juridisko personu, ja:

- 1) pārzinis ir reģistrēts Latvijas Republikā;
- 2) datu apstrāde tiek veikta ārpus Latvijas Republikas robežām teritorijās, kas pieder Latvijas Republikai saskaņā ar starptautiskajiem līgumiem;
- 3) Latvijas Republikā atrodas aprīkojums, kas tiek izmantots personas datu apstrādei, izņemot gadījumus, kad aprīkojums tiek izmantots tikai personas datu pārraidei caur Latvijas Republikas teritoriju.

Fizisko personu datu aizsardzības likums neattiecas uz personas datu apstrādi, ko fiziskās personas veic personiskām vai mājas un ģimenes vajadzībām, pie nosacījuma, ja personas dati netiek izpausti trešajām personām. Piemēram, elektroniskās piezīmju grāmatiņas, adrešu grāmatas, ģimenes foto albūmi, ģimeņu mājas lapas ar ierobežotu pieeju.

Tāpat likums neattiecas uz juridisko personu datiem, piemēram, juridisko personu nosaukumiem, izņemot gadījumus, ja tas ietver fiziskas personas vārdu.

**Personas datu apstrāde** - jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu. Piemēram, skolēnu un skolas darbinieku personas lietu veidošana, dažādas informācijas ievade skolu informācijas sistēmās, u.t.t.

**Personas dati** - jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu. Piemēram, vārds, uzvārds, personas kods, telefona numurs, fotogrāfijas, pirkstu nospiedumi, dzīvesvietas adrese, dzimums, vecums, u.t.t. Ne vienmēr šāda informācija ir tieši sasaistīta ar personas vārdu,

uzvārdu, bet gan var tikt saistīta ar personu, lai identificētu un uzzinātu par personas paradumiem. Sīkāk skatīt Datu valsts inspekcijas rekomendācija "Personas datu definīcija". Piemēram, persona ar personas kodu XXXXXX-XXXXX apmeklē ārstu vienreiz mēnesī.

**Pārzinis** — fiziska vai juridiska persona, valsts vai pašvaldību institūcija, kura nosaka personas datu apstrādes (vākšanas, reģistrācijas, pārveidošanas, u.c.) mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar likumu.

Pārzinim ir pienākums nodrošināt personas datu aizsardzības principu ieviešanu, pēc pieprasījuma jāinformē personas par to pieejas tiesībām personas datiem, tiesībām tos labot, kā arī likumā noteiktos gadījumos jāreģistrē personas datu apstrāde Datu valsts inspekcijā (turpmāk - inspekcija).

Pārzinis var uzticēt personas datu apstrādi **personas datu operatoram**, noslēdzot rakstveida līgumu. Personas datu operators var apstrādāt personas datus tikai, lai izpildītu līgumu, un tikai saskaņā ar pārziņa norādījumiem. Piemēram, ja skolas Interneta mājas lapu uztur ārpalpojumu sniedzējs, tad likuma izpratnē tas ir personas datu operators.

### **Personas datu aizsardzības principi**

Skolu rīcībā esošie personas dati, kas tiek apstrādāti, lai izpildītu skolu funkcijas, ir jāaizsargā, jo tā ir daļa no personu privātuma un tās izpaušana var aizskart datu subjektu tiesības.

Likums nosaka personas datu apstrādes nosacījumus un noteikumus. Likums arī nosaka to personu tiesības, kuru dati tiek apstrādāti.

Skolu pienākums ir nodrošināt personas datu aizsardzību, un tā kontekstā svarīgs ir caurskatāmības un personu (skolēnu, darbinieku) uzticēšanās aspekts. Skolu direktoram ir jānodrošina, ka katram personas datu veidam ir noteikts un skaidrs apstrādes mērķis, ka ir skaidri noteikts, kādos gadījumos var tikt nodoti personas dati citām personām un iestādēm, kā arī jānodrošina, ka personas dati ir drošībā un aizsargāti.

### **Personas datu apstrādes mērķa noteikšana**

Personas datus var apstrādāt tikai likumīgam un iepriekš noteiktam mērķim, kas saistīts ar skolu funkciju izpildi. Skolas direktors atbild par šādu mērķu noteikšanu (izņemot, ja datu apstrādes mērķis noteikts normatīvajos

aktos), to ieviešanu un izpildes kontroli. Piemēram, skolēnu dati nevar tikt izmantoti komerciāliem vai politiskiem mērķiem, ja vien nav iegūta atbilstoša piekrišana personas datu izmantošanai iepriekš minētajiem mērķiem.

### **Proporcionalitātes princips**

Ir tiesības apstrādāt tikai tādas personas datus, kas nepieciešami noteikta mērķa sasniegšanai. Piemēram, pieprasīt informāciju par skolēna vecāku ienākumiem nav atbilstoši, jo tas nav saistīts ar mērķa sasniegšanu - skolu funkciju izpildi.

### **Personas datu apstrādes ilgums**

Datu apstrādes ilgumam jābūt saistītam ar noteiktu personas datu apstrādes mērķi. Piemēram, informācija, kas tiek apstrādāta saistībā ar eksāmeniem, var tikt apstrādāta tikai tik ilgi, kamēr tas ir nepieciešams saistībā ar eksāmena norisi. Personas datiem, kas tiek arhivēti, ir jābūt nošķirti no citiem personas datiem. Piemēram, atsevišķā datu nesējā.

### **Personas datu drošība**

Skolas direktoram ir jānodrošina personas datu drošība, t.i., tam ir pienākums nodrošināt datu konfidencialitāti un nodrošināt, lai dati nelikumīgi nenokļūtu trešo personu rīcībā.

Tāpat ir jānodrošina, ka personas datiem var piekļūt tikai tam pilnvaroti darbinieki, ja to darba pienākumi ir saistīti ar noteikto personas datu apstrādi. Piemēram, jānodrošina, ka katram lietotājam, kurš piekļūst personas datiem, ir individuāla parole, kas tiek regulāri mainīta, un ir precīzi noteikts, kādiem datiem konkrētam lietotājam (darbiniekam, vecākiem, skolēniem, palīgpersonām) ir nepieciešams piekļūt.

Ir jānodrošina, ka personas datus nevar sagrozīt, bojāt un tiem nepieklūst nepilnvarotas personas. Piemēram, ārpakalpojumu sniedzēju gadījumos, līgumos ir jānosaka to atbildība par datu drošību.

Skolas direktoram ir jānodrošina, ka ir ieviesti atbilstoši drošības pasākumi un līdzekļi, t.i., gan loģiskie, gan fiziskie drošības līdzekļi. Piemēram,

- telpām - atbilstoši ugunsdrošības pasākumi, ierobežota piekļuve dokumentiem, apsardze, signalizācija;
- informācijas tehnoloģijām un datiem: rezerves kopijas, uzstādīta antivīrusa programmatūra, regulāri tiek mainīta parole, kas sastāv ne

mazāk kā no 8 simboliem.

Drošības pasākumiem ir jābūt atbilstošiem apstrādātajiem personas datu veidiem un to riskiem. Piemēram, jābūt augstam autentifikācijas (lietotāja identitātes pārbaude) līmenim attiecībā uz piekļūšanu testu (jeb pārbaudījumu, ieskaitu, eksāmenu) rezultātiem, sensitīvus personas datus (t.i. personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi) var nosūtīt pa Internetu, ja ir nodrošināta datu šifrēšana.

### **Datu subjektu tiesību ievērošana**

#### **a) Datu subjektu informēšana**

Datu subjekts - fiziskā persona, kuru var tieši vai netieši identificēt. Piemēram, skolēni, skolēnu vecāki, skolu darbinieki.

Pirms personas datu ievākšanas datu subjekti ir jāinformē par datu apstrādes mērķi, pārzini un par personas datu operatoru, ja tāds ir. Piemēram, izmantojot anketas personas datu ievākšanai, vienlaicīgi ir jāsniedz informācija mutiski vai tai jābūt iekļautai anketā par to, kas ir pārzinis minētajai datu apstrādei (atbildīgais par datu apstrādi), kas ir personas datu operators un kāds ir personas datu apstrādes mērķis (t.i., kādam nolūkam dati tiek vākti).

Vēlams, vienlaicīgi ir informēt datu subjektu arī par iespējamiem personas datu saņēmējiem, par iespējām un kārtību datu subjektam piekļūt saviem personas datiem, kā arī izdarīt labojumus tajos, kā arī vai personas datu sniegšana ir obligāta vai brīvprātīga. Šādu informāciju, piemēram, var sniegt gan izmantojot atsevišķas veidlapas, gan ievietojot informāciju iestādes Interneta mājas lapā, kā arī nosūtot vēstules personām, kuru dati tiek apstrādāti.

#### **b) Datu subjektu pieejas tiesības un datu labošana**

Jebkurš datu subjekts vai viņa pārstāvis (skolēns, skolēnu vecāki, kas pārstāv skolēnus, skolotāji, skolu darbinieki) var pieprasīt jebkuru informāciju par sevi (datu subjektu), kas ir iestādes rīcībā, kā arī viņam ir tiesības pieprasīt tos labot vai dzēst, ja dati ir nepilnīgi, novecojuši, nepatiesi, pretlikumīgi iegūti vai arī tie vairs nav nepieciešami vākšanas mērķim.

### **Datu izpaušana par skolēnu trešajām personām**

Izpaūžot personas datus par skolēnu trešajām personām, būtu ieteicams

ievērot, ka pieprasījumam iegūt personas datus ir jābūt noformulētam rakstveida iesniegumā (vai iesniegumam jābūt parakstītam ar drošu elektronisko parakstu). Piemēram, ja datus pieprasa policija, tiesa, arī nepieciešams saņemt rakstveida informācijas pieprasījumu, lai varētu identificēt informācijas pieprasītāju. Ja speciālie normatīvie akti neparedz tiesības trešajām personām iegūt personas datus, bet trešā persona lūdz informāciju par skolēnu, tad Jūs varat jautāt vecākiem, vai viņi piekrīt, ka Jūs izpaužat personas datus par skolēnu vai vecākiem. Piemēram, futbola klubs varētu vēlēties noskaidrot skolas talantīgākos futbolistus, lai izskatītu iespēju uzaicināt viņus spēlēt savā futbola klubā. Šādā gadījumā personas datu nodošanai klubam nepieciešama konkrēto skolēnu vecāku piekrišana.

### **Datu valsts inspekcijas loma datu aizsardzībā**

Datu valsts inspekcija ir valsts pārvaldes iestāde, kas veic personas datu aizsardzības uzraudzību. Tā darbojas neatkarīgi un patstāvīgi, izpildot normatīvajos aktos noteiktās funkcijas, pieņem lēmumus un izdod administratīvos aktus saskaņā ar likumu.

#### **Datu valsts inspekcijas funkcijas un tiesības:**

1. Kontrolēt personas datu apstrādes atbilstību Fizisko personu datu aizsardzības likumam. Inspekcija veic arī pirmsreģistrācijas pārbaudes atsevišķās riska jomās, saņemot personas datu apstrādes reģistrācijas iesniegumus.

2. Sūdzību izskatīšana. Inspekcija saņem sūdzības no jebkuras personas par iespējamiem datu apstrādes aizsardzības pārkāpumiem. Inspekcija var pieprasīt datu bloķēšanu, kļūdainu vai nelikumīgi iegūtu datu izdzēšanu vai iznīcināšanu, noteikt pastāvīgu vai pagaidu aizliegumu datu apstrādei, kā arī, ja saskata noziedzīga nodarījuma (Krimināllikuma 145.pants) pazīmes, nosūta informāciju prokuratūrai.

3. Inspekcija veic personas datu apstrādes pārbaudes uz vietas. Inspekcijai ir tiesības brīvi apmeklēt jebkuras nedzīvojamās telpas, kurās atrodas personas datu apstrādes, un pārziņa pārstāvja klātbūtnē veikt nepieciešamo pārbaudi vai citus pasākumus, lai noteiktu personas datu apstrādes procesa atbilstību likumam. Inspekcijas darbinieki var pieprasīt rakstveida vai mutvārdu paskaidrojumus no jebkuras fiziskās vai juridiskās personas, kas saistīta ar personas datu apstrādi, pieprasīt, lai tiek uzrādīti dokumenti un sniegta cita informācija, kas attiecas uz pārbaudāmo personas datu apstrādi, kā arī pieprasīt personas datu apstrādes, jebkuras tās iekārtas vai informācijas

nesēja pārbaudi un noteikt ekspertīzi pārbaudāmo jautājumu izpētei.

4. Tiesības piemērot sankcijas. Likumā noteiktajā kārtībā Inspekcijai ir tiesības uzlikt administratīvos sodus par pārkāpumiem personas datu apstrādē (brīdinājums, naudas sods līdz desmit tūkstoš latiem, konfiscējot pārkāpuma priekšmetus un izdarīšanas rīkus vai bez konfiskācijas), pieprasīt datu bloķēšanu, kļūdainu vai nelikumīgi iegūtu datu izdzēšanu vai iznīcināšanu, noteikt pastāvīgu vai pagaidu aizliegumu datu apstrādei.

## **Praktiskās rekomendācijas attiecībā uz personas datu apstrādi skolās**

### **Personas koda apstrāde**

Personas kodu drīkst apstrādāt (jeb izmantot), ja ir datu subjekta piekrišana, ja personas kodu apstrāde ir nepieciešama, lai sasniegtu noteiktu personas datu apstrādes mērķi, vai arī, ja ir saņemta Inspekcijas atļauja. Piemēram, ir pieļaujams apstrādāt personas kodus skolēnu lietās, lai identificētu noteiktu skolēnu. Savukārt, ir vērtējams, vai personas kods ir nepieciešams, veicot kādu aptauju vai anketēšanu skolās, kā arī lai reģistrētu skolēnu skolas bibliotēkā kā lasītāju.

### **Personas fotogrāfija**

Personas vai personu grupas fotogrāfijas izmantošana ir vispārēja prakse skolās. Piemēram, pievienojot tos skolēnu dokumentiem, publicējot tos skolu informatīvajos materiālos, skolu avīzēs, Interneta mājas lapās, vai izvietojot tās publiski skolas telpās.

Kāpēc jāaizsargā personas fotogrāfija? Personas attēls ir uzskatāms par personības raksturīgu pazīmi un tas ir privātās dzīves konfidencialitātes elements un tam jābūt aizsargātam, ņemot vērā personu tiesības uz to, ka viņu privātā dzīve tiek respektēta. Fotogrāfijas izmantošanai ir jābūt stingri noteiktai, jebkuram datu subjektam attiecībā uz viņa fotogrāfiju ir ekskluzīvas tiesības uz tās izplatīšanu, kā arī persona var iebilst pret fotogrāfijas izmantošanu vai izplatīšanu bez tās piekrišanas.

### **Kas jāievēro fotografējot skolā?**

Jābūt ir vienošanās ar personu, kas tiek fotografēta. Piemēram, skolas izstrādā iekšējo kārtību par fotografēšanu un/vai filmēšanu skolās, kur iekļauj kārtību, kādā vecāki tiek informēti, kad bērni var tikt skolā fotografēti, kā un kad

vecāki var pret to iebilst, kā un kur fotogrāfijas var tikt publiskotas.

Likums neaizliedz vecākiem fotografēt skolā dažādus pasākumus, piemēram, Ziemassvētku pasākumu vai sporta dienas, bet fotogrāfijas nevar tikt publiskotas.

Personu fotografēšanai un fotogrāfiju izplatīšanai ir jānotiek saskaņā ar personas tiesībām uz savu attēlu. Jebkurš var iebilst pret sava attēla izmantošanu jebkādā formā (izmantošanu skolu Intranetā, Internetā, u.t.t.).

Skolas pienākums ir nodrošināt nepieciešamo piekrišanu fotogrāfiju izmantošanai. Piemēram, ja tiek plānots, ka skolas pasākuma laikā tiks veikta fotografēšana, lai sniegtu informāciju par iestādes darbu, un pēc tam fotogrāfijas tiks izvietotas skolas avīzē, Internetā, u.c. Inspekcija, iesaka, prasīt atļauju skolēnu vecākiem, lai izvietotu viņu bērnu fotogrāfijas publiski, izmantojot, piemēram, noteiktas veidlapas. Inspekcija atgādina, ka personām ir tiesības piekļūt saviem datiem (t.sk. savām fotogrāfijām), pieprasīt tos dzēst vai iznīcināt. Šāds situācijas risinājums attiecināms arī tad, ja skolā vēlmi filmēt izsaka žurnālisti.

### **Skolēnu datu apstrāde izmantojot Internetu**

Pastāv vairāki portāli vai sistēmas, kas nodrošina, ka skolēna datiem var piekļūt izmantojot Internetu. Piemēram, portāls *E-klase*.

- Šai gadījumā atsevišķa uzmanība ir jāpievērš tieši tehniskajiem drošības jautājumiem. Piemēram, ir jānodrošina, ka katrs lietotājs var piekļūt tikai tiem datiem, kas attiecas uz viņu vai saistīts ar viņa amata (darba) pienākumiem. Skolēns, skolēna vecāki nedrīkst piekļūt datiem par citiem skolēniem. Tāpat pieejas parolēm jābūt droši veidotām, piemēram, tām jā sastāv ne mazāk kā no 8 simboliem, tās nevar tikt glabātas tiešā tekstā, u.t.t. Tāpat sistēmas lietotājiem jābūt zinošiem par sistēmas konfidencialitātes jautājumiem.
- Nepieciešams informēt lietotājus par to tiesībām saskaņā ar Fizisko personu datu aizsardzības likumu.

Šādai informācijai ir jābūt pieejamai attiecīgajā mājas lapā, kā arī jābūt pieejamai tai brīdi, kad tiek veidots lietotāja konts. Katram lietotājam ir jābūt pieejai tikai tiem datiem, kuri ir nepieciešami, lai izpildītu savus darba/amata pienākumus skolā. Katram datu subjektam ir tiesības piekļūt saviem datiem, tos labot, pieprasīt dzēst saskaņā ar Fizisko personu datu aizsardzības likumu.

## **Lietotāja datora kontrole**

Lai nodrošinātu tīkla un/vai tehnisko resursu (piemēram, datora) drošību, ir jāievieš to lietošanas kontrole. Šāda kontrole ir tiesiska, ja ir nodrošināta tās caurspīdīgums, informējot par to lietotājus. Ir skaidri jānosaka abu pušu (skolas un lietotāju) pienākumi, informējot par kontroles nosacījumiem un sankcijām lietotājiem, ja tie neievēros lietošanas noteikumus. Šie noteikumi īpaši ir jāņem vērā attiecībā uz skolas darbinieku darba elektronisko pastu un Interneta lietošanu darba vietā.

## **Mācību novērtējuma izpaušana**

Skolām ir jānodrošina, ka katra skolēna novērtējums (arī dažādas piezīmes attiecībā uz skolēnu mācību procesu) ir pieejamas tikai pašam skolēnam vai tā likumīgam pārstāvim (piemēram, vecākiem).

## **Statistikas dati un citi pētījumi**

Lielākajā daļā gadījumu statistikas datu iegūšanai personas dati nav vajadzīgi.

Pētījumos bieži tiek izmantoti dažādi skolnieku personas dati, kas iegūti no vairāk vai mazāk detalizētām aptaujas anketām. Šo datu (jo īpaši sensitīvo personas datu) vākšanai ir jāsaņem bērna likumīgo pārstāvju atļauja, un bērna pārstāvji ir jāinformē par pētījuma nolūku un datu saņēmējiem. Turklāt, ja iespējams, pētījumi ir jāizstrādā bez bērnu identitātes atklāšanas.

## **Biometrijas datu izmantošana**

Biometrijas datu apstrāde ietver sevī dažādu informācijas tehnoloģiju lietošanu, ar kuru palīdzību var tikt identificēta persona, izmantojot personas fiziskos, bioloģiskos vai paradumu rādītājus (sejas vai rokas kontūras vai forma, acs tīklenes attēls, pirkstu un delnu pēdas nospiedumi, DNS, u.t.t.) Biometrijas dati ir personas dati, jo tie identificē personu. Biometrijas dati pamatā tiek lietoti, lai nodrošinātu telpu pieejas drošību.

Tā kā pastāv potenciāli draudi saistībā ar minēto rādītāju apstrādi, kuri ir unikāli katrai personai, un daži (pirkstu nospiedumi, DNS, u.c.) var tikt ievākti, personai to nezinot, tad šādu datu apstrāde ir jāreģistrē Datu valsts inspekcijā.

Attiecībā uz šo datu apstrādi ir jābūt ieviestiem īpašiem drošības pasākumiem attiecībā uz kopēju datu bāzi, kur tiek apstrādāti minētie dati, vai

arī attiecībā uz ierīci, kur glabājas dati.

Ieviešot skolās biometrijas datu apstrādi, ir jāveic risku izvērtēšana, izvērtējot nepieciešamību izmantot personu biometrijas datus, lai sasniegtu paredzēto mērķi, u.t.t. Detalizētāku informāciju par biometrijas datu apstrādes ieviešanu, skatīt nodaļā par videonovērošanu skolās.

### **Videonovērošana skolās**

Videonovērošana pārsvarā tiek izmantota, lai nodrošinātu aizsardzību pret ļaunprātīgu rīcību vai noziedzīgiem nodarījumiem. Videonovērošanas veikšana ietekmē personas brīvības (piemēram, brīvību nākt un iet). Līdz ar to ir nepieciešams ieviest atbilstošus personas datu aizsardzības noteikumus.

1. Pirms videonovērošanas kameru uzstādīšanas ir jāveic risku izvērtēšana, ņemot vērā dažādu incidentu raksturu, kas notiek skolas teritorijā. Tas palīdzēs identificēt alternatīvus risinājuma veidus, lai sasniegtu mērķus, iespējams, neizmantojot videonovērošanu. Piemēram, drošu iekļūšanu skolā var nodrošināt, izmantojot magnētiskās kartes.

2. Proporcionalitātes princips. Ja videonovērošanas ieviešana atbilst sasniedzamajiem drošības mērķiem (telpu piekļūšanas kontrole), tas vienlaicīgi nevar būt mērķis, lai novērotu noteiktus darbiniekus vai noteiktu personu grupas, kas nav saistīti ar drošības mērķiem. Videokameru skaits, izvietojums, novērošanas perimetrs, kameru funkcijas un kameru darbības periodiskums, vai novēroto personu pienākumi ir visi tie faktori, kas jāņem vērā, kad tiek novērtēta videonovērošanas proporcionalitāte.

Piemēram, videonovērošanas sistēmas iespējams var būt nelikumīgas, ja sistēma ir izvietota telpās, kur jāpieļauj personu privātums (tualetes, dušas, apģērbu maiņas telpas, skolas medicīniskās aprūpes kabinets).

- *Pienākums informēt*

Nav pieļaujama jebkāda novērošana bez personu (skolotāju, skolēnu, darbinieku un apmeklētāju) informēšanas.

Par videonovērošanu jebkura persona, kas tiek filmēta vai var tikt filmēta, ir jāinformē skaidrā un saprotamā veidā, piemēram, izvietojot brīdinājuma zīmes pie ieejas telpās vai teritorijā.

- *Atbilstošu dokumentu izstrāde*

Ir vēlams, ka iestādes dokumentos ir skaidri identificēti videonovērošanas mērķi un kārtība, kādā personas var piekļūt videonovērošanas attēliem, kā arī jānosaka šo personu tiesības un jānodrošina atbilstoša apmācība. Turklāt ir

jānosaka attēlu uzglabāšanas laiks un noteiktas procedūras, kas reglamentē pieejas tiesības attēliem.

- *Pieklūve attēliem ir ierobežotam noteiktu personu lokam*

Attēliem var piekļūt tikai tās personas, kuras tam ir speciāli pilnvarotas un kurām ir atbilstoši pienākumi (piemēram, drošības struktūrvienības vadītājam, atbildīgajai personai par drošību skolās). Šīm personām ir jābūt apmācītām un jāpārzina videonovērošanas kārtība un tās datu aizsardzība.

- *Videonovērošanas attēlu uzglabāšanas laiks*

Ierakstu ilgums nevar pārsniegt **dažas dienas** un ieraksti ir jāiznīcina pēc šī perioda, izņemot gadījumus, ja tiek veikta izmeklēšana vai saņemts tiesībaizsardzības iestāžu rakstisks informācijas pieprasījums. Šis periods jebkurā gadījumā nevajadzētu pārsniegt **mēnesi**.

- *Jāievēro noteiktas formalitātes pirms videonovērošanas ieviešanas*

Videonovērošana nevar tikt uzsākta pirms tā nav reģistrēta Datu valsts inspekcijā.

### **Skolu mājas lapu veidošana internetā**

Skolu interneta mājas lapas ir kļuvušas par daļu no skolas ikdienas dzīves. Tā kā tā ir izvietota Internetā, tad tā ir pieejama publiski.

Papildus, informācijas meklētāju rīki kļūst aizvien efektīgāki, tādējādi palielinot risku, ka var tikt aizskarts personu privātums. Izmantojot personas vārdu, ir iespēja izveidot personas “virtuālo” biogrāfiju, piemēram, iegūstot informāciju par skolēna dalību ārpuskolas pasākumos un dalību citās sabiedriskās aktivitātēs.

Līdz ar to, Interneta mājas lapu veidošanā un uzturēšanā ir jāievēro personas datu aizsardzības prasības. Personas dati var tikt izvietoti mājas lapā tikai saskaņā ar Fizisko personu datu aizsardzības likumā noteikto. Tāpat var tikt sodītas darbības, ja mājas lapā tiek izplatīta godu un cieņu aizskaroša vai rasistiska informācija.

Lai vāktu personas datus (piemēram, pieteiktos informatīvā biļetena saņemšanai), personām, no kurām informācija tiek vākta, ir jābūt informētām par datu vākšanas mērķi, un, pēc pieprasījuma, par datu saņēmējiem un piekļuves tiesībām, tiesībām labot datus un tiesībām prasīt dzēst datus.

### **Skolu blogi (*emuāri*)**

Šai gadījumā ar vārdu “*blogs*” tiek saprastas personu veidotas tīmekļa

vietnes, kā žurnāls vai personisku interešu prezentācija (piemēram, par sportu, kultūru, ideju apmaiņa, u.c.)

Blogs nav vietne, kur persona var jebko izvietot/publiskot, neievērojot likuma noteikumus. Ir jāievēro noteikti noteikumi un citu personu tiesības. Līdz ar to katram blogerim ir jāapzinās, ko var darīt un ko nē.

Vecāki ir atbildīgi par savu bērnu publikācijām. Pieļaujams, ka vecāki dod atļauju saviem nepilngadīgajiem (līdz 18 gadu vecumam) bērniem veidot savu blogu.

Civillikuma 177.pants nosaka, ka rūpes par bērnu nozīmē viņa aprūpi, uzraudzību un tiesības noteikt viņa dzīvesvietu. Savukārt, bērna uzraudzība nozīmē rūpes par bērna paša drošību un trešās personas apdraudējuma novēršanu. Vienlaicīgi nepilngadīgajam var tikt piemērota administratīvā vai kriminālatbildība no 14 gadu vecuma, ja tas nelikumīgi apstrādā personas datus. Piemēram, praksē tas nozīmē, ka vecāki atbild, ja to nepilngadīgais bērns izvieto bez atļaujas citu personu attēlus internetā. Ja tiek konstatēts, ka nepilngadīgais nelikumīgi veicis datu apstrādi, tad, ja personai nodarīts kaitējums vai radīti zaudējumi, tai ir tiesības saņemt atbilstīgu atlīdzinājumu. Minētās atlīdzināšanas pienākums ir nepilngadīgā (līdz 18 gadu vecumam) vecākiem.

Vai var tikt publicētas sava bērna draugu vai skolotāju fotogrāfijas? Tās var tikt izvietotas, ja persona pret neiebilst.

Izvietojot blogā godu un cieņu aizskarošu informāciju, vai informāciju, kuru saskaņā ar likumu ir aizliegts izplatīt (piemēram, rasistiska rakstura), skolotājs vai skolēns var tikt saukts pie administratīvās vai kriminālatbildības. Nepilngadīgajam var tikt piemērota administratīvā vai kriminālatbildība no 14 gadu vecuma.

### **Sava privātuma aizsardzība Internetā**

Ir jāapzinās, ka Internetā visas darbības, ieskaitot informācijas meklēšanas ierīču izmantošana, atstāj "pēdas". Līdz ar to ir pilnīgi neiespējami pilnībā dzēst informāciju. Aplūkojot Interneta mājas lapas, tiek saglabāta informācija, ko pieļauj lietotāja dators: tas atstāj lietotāja datora "pēdas".

Tāpat katra darbība, izmantojot interneta meklēšanas rīkus, tiek saglabāta: lietotāja datora IP adrese, informācija, kas ir sīkdatnē (*cookies*), meklēšanas atslēgas vārdi un saite, ko mēs izmantojām, lai atvērtu atrasto mājas lapu. Līdz ar to meklēšanas ierīču uzturētāji precīzi zina lietotāja interneta lietošanas paradumus.

Līdz ar to liels informācijas apjoms par personu paradumiem ir pieejams internetā, tādas kā personu politiskie uzskati, informācija par personu seksuālo

dzīvi, informācija par personu attiecībām ir pieejamas blogos. Ir pieejami Internetā arī videorulliši, kur bieži ir ievietota informācija personai to nezinot.

Tāpat bērni bieži ir ideāls mērķis/avots, lai negodprātīgi iegūtu informāciju par viņiem un viņu ģimenēm. Informācijas apmaiņas ātrums, interaktivitāte un pat spēļu elementa klātesamība padara bērnus par ideālu mērķi, lai iegūtu daudz vairāk un precīzāku informāciju.

Attiecībā uz iepriekš minēto likums nosaka, ka personas dati ir informācija, kas attiecas uz identificētu vai identificējamu fizisko personu, piemēram, personas vārds, uzvārds, personas fotogrāfija, mobilā telefona numurs, IP adrese, ko zina jūsu interneta pakalpojumu sniedzējs, u.t.t.

Likums nosaka, ka personas datiem jābūt saglabātiem pēc iespējas īsāku laika periodu attiecībā uz datu glabāšanas mērķa sasniegšanu. Datu saglabāšanas ilguma kontekstā ir jāpastāv "tiesībām tikt aizmirstam". Ko nozīmē "tiesības tikt aizmirstam"? Cilvēka smadzenēm piemīt spēja aizmirst informāciju, ko tās ir ieguvušas. Bet tas neattiecas uz datoru. It īpaši "tiesībām tikt aizmirstam" Interneta vidē ir svarīga nozīme. Protams, Interneta vidē tas ir nosacīti. Līdz ar to vislabākais veids aizsargāt sevi ir pievērst uzmanību tam, kas tiek publicēts Internetā. Tas praksē ir grūti, jo sociālie tīkli aizvien vairāk atklāj informāciju par personu, personai nezinot, kas ir piekļuvis šādai informācijai, kādiem mērķiem un cik ilgi par viņu tiek saglabāta informācija. Šāda informācija tiek izmantota aizvien ātrāk un ātrāk, lielākā apjomā, un ir potenciāli pieejama visā pasaulē. Nevienam nevar kontrolēt informāciju, kas ir izvietota internetā. Tāpēc ir svarīgi ievērot piesardzību, publicējot internetā informāciju. Internetā "pēdas" saglabājas ļoti ilgi un tāda datu apstrāde ir kā "laika deglis", piemēram, darbā iekārtošanās procesā, kas var ietekmēt indivīda dzīvi arī pēc vairākiem gadiem pēc informācijas publiskošanas internetā.

Ņemot vērā minēto, ir 10 ieteikumi savai personas datu aizsardzībai Internetā. **Pirms publicējiet, padomājiet!**

1. Uzdodiet tos pašus jautājumus, ko Jūs iespējams jautātu "reālajā dzīvē", izpaužot informāciju par sevi. Piemēram, vai es vēlos, lai manas fotogrāfijas ar draugiem būtu pieejamas maniem vecākiem vai skolotājiem, kā arī visiem interneta lietotājiem?
2. Internetā pieejamās informācijas apjoms par Jums, pirmkārt, ir atkarīgs no tā, cik daudz Jūs pats publicējat to Internetā.
3. Jābūt modram, esot sociālajos tīklos: sniedziet par sevi pēc iespējas mazāk informācijas vai tik maz, cik maz ir pieļaujams.
4. Pirms sākat lietot noteiktu sociālo tīklu, izlasiet informāciju, kā varat ietekmēt sava profila informāciju. Veidojot savu profilu sociālajā tīklā,

ierobežojiet tam piekļuvi, bet ja Jums jau ir savs profils, tad atcerieties, ka jāierobežo to personu loks, kas var redzēt informāciju par Jums (Jūsu ievietoto tekstu, fotogrāfijas, video sociālajā tīklā). Iestatījumi pieļauj ierobežot piekļūšanu Jūsu personas datiem noteiktam personu (t.i. visu Jūsu draugu vai tikai dažu draugu) lokam. Piemēram, ierobežojiet, ka meklēšanas ierīces indeksēs (izmantos) Jūsu profilā esošo informāciju, līdz ar to Jūs varēsiet kontrolēt savu informāciju un, ja vēlēšities, to arī dzēst.

5. Kontrolējiet savas darbības blogā, dažādos forumos, Facebookā, Twitterī.
6. Nepublicējiet fotogrāfijas. Piemēram, apdomājiet, ja Jūs šodien dariet pieejamas savas fotogrāfijas saviem draugiem, kas notiks, ja rīt kāds no Jūsu draugiem vairs nebūs Jūsu draugs un izplatīs visiem Jūsu fotogrāfijas.
7. Nepubliskojiet informāciju internetā, kas var ietekmēt un aizskart citas personas. Nedariet citām personām to, ko Jūs nevēlaties, lai citas personas nodara Jums.
8. Pārbaudiet regulāri, kas par Jums ir publicēts Internetā. Piemēram, ierakstot Jūsu vārdu meklēšanas ierīcēs, Jūs varat iegūt informāciju par to, kāda informācija par Jums ir pieejama. Jūs varat prasīt mājas lapas uzturētājam, lai informācija par Jums tiktu dzēsta, kā arī lai tiktu dzēsta informācija, kas ir tikusi saglabāta meklēšanas ierīcē.
9. Ja iespējams, lietojiet pseidonīmus, kas Jūs neidentificē.
10. Nepadariet pieejamas Jūsu paroles un neizvēlaties paroles, kas ir ļoti vienkāršas (piemēram, dzimšanas datums vai ģimenes locekļu vārdi). Izvēlieties dažādas paroles katrai mājas lapai. Atcerieties izslēgt Jūsu datoru vai aizvērt Jūsu profilu, kad Jūs vairs nestrādājat ar datoru.

### **Personas datu apstrādes reģistrācija Datu valsts inspekcijā**

Skolām, veicot skolēnu (audzēkņu) un pedagogu personas datu apstrādi saskaņā ar Izglītības likumu (t.i. skolēnu lietas, sekmju žurnāli, pedagogu uzskaitē) nav jāreģistrē personas datu apstrāde Datu valsts inspekcijā. Ņemot vērā likuma „Par pašvaldībām” 5.panta otro daļu (pašvaldība atbild par tās izveidoto institūciju darbību, ja likumos nav noteikts citādi), 7.panta otro daļu (likuma „Par pašvaldībām” 15.pantā paredzēto autonomo funkciju izpildi organizē un par to atbild pašvaldības) un 15.panta 4.punktu, kas nosaka pašvaldībām funkciju - gādāt par iedzīvotāju izglītību, personas datu apstrādes reģistrācija Datu valsts inspekcijā ir jāveic pašvaldībām, norādot vispārējās izglītības iestādes kā personas datu apstrādes vietas.

**Datu valsts inspekcija**  
**Tālrunis: 67223131**  
**Blaumaņa iela 11/13-15**  
**Rīga, LV-1011**  
**e-pasta adrese: [info@dvi.gov.lv](mailto:info@dvi.gov.lv)**  
**[www.dvi.gov.lv](http://www.dvi.gov.lv)**