

A graphic of a barcode with vertical bars of varying heights. The central portion of the barcode is highlighted in green, serving as a background for the title text.

Rekomendācija

«Bērnu datu aizsardzība skolās»

Rīga

Ievads

Bērnam ir tiesības brīvi izteikt savas domas; šīs tiesības ietver brīvību meklēt, saņemt un nodot jebkāda veida informāciju un idejas neatkarīgi no robežām mutvārdos, rakstveidā vai drukātā veidā, mākslas darbu veidā vai ar citu līdzekļu palīdzību pēc bērna izvēles.¹

Neviens bērns nedrīkst būt patvaļīgas vai nelikumīgas iejaukšanās viņa tiesību realizēšanā uz personisko dzīvi, ģimenes dzīvi, dzīvojamo telpu neaizskaramību vai korespondences noslēpumu vai viņa goda un reputācijas nelikumīga apdraudējuma objekts.²

Bērna tiesības un brīvības valsts nodrošina visiem bērniem bez jebkādas diskriminācijas – neatkarīgi no bērna, viņa vecāku, aizbildņu, ģimenes locekļu rases, tautības, dzimuma, valodas, partijas piederības, politiskās un reliģiskās pārliecības, nacionālās, etniskās vai sociālās izcelsmes, dzīvesvietas valstī, mantiskā un veselības stāvokļa, dzimšanas vai citiem apstākļiem.³

Bērnu tiesību aizsardzība, tajā skaitā tiesības uz privātumu un personas datu aizsardzību, nosaka dažādi normatīvie akti. Tomēr, salīdzinājumā ar pieaugušajiem, bērni ir īpašā situācijā – ne visas savas tiesības (arī savas kā datu subjekta tiesības) viņi līdz 18 gadu vecuma sasniegšanai var izmantot nepastarpināti (t.i., bez vecāku vai pilnvarotas personas starpniecības). Bērni ne vienmēr ir arī pietiekami informēti par savām tiesībām, spēj izvērtēt savu rīcību un paredzēt tās se-

kas. Tādēļ īpaša uzmanība ir jāpievērš bērnu informēšanai, lai pēc iespējas novērstu riskus un nelikumīgas personas datu apstrādes iespējas.

Visās darbībās attiecībā uz bērniem neatkarīgi no tā, vai tās veic valsts iestādes vai privātiestādes, kas nodarbojas ar sociālās nodrošināšanas jautājumiem, tiesas, administratīvie vai likumdošanas orgāni, uzmanība pirmām kārtām tiek veltīta tam, lai vislabāk nodrošinātu bērna intereses.⁴ Šāds princips attiecināms arī uz bērnu datu aizsardzības nodrošināšanu skolās.

Palielinoties informācijas apjomam, kas ir skolu rīcībā, kā arī (īpaši ņemot vērā arī bērnu aktīvo informācijas tehnoloģiju izmantošanu), aizvien vairāk uzmanības 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 aktualizēt personas datu aizsardzības jautājumu skolās un sniegt atbildes uz jautājumiem, kas attiecas uz bērnu personas datu aizsardzību skolās, īpaši respektējot bērnu tiesības attiecībā uz privātumu.

1 ANO Konvencija par bērnu tiesībām, 13. panta pirmais punkts.

2 ANO Konvencija par bērnu tiesībām, 16. panta pirmais punkts.

3 Bērnu tiesību aizsardzības likuma 3. panta otrā daļa.

4 ANO Konvencija par bērnu tiesībām, 3. panta pirmais punkts.



Rekomendācija ir informatīvs materiāls, tai ir ieteikuma raksturs, un tās mērķauditorija ir vecāki, pedagogi un izglītības iestāžu darbinieki, kā arī skolēni un pašvaldību pārstāvji, kuru kompetencē ietilpst bērnu datu apstrādes skolās, un ārpusstabilas interešu centru pārstāvji. Tomēr rekomendācija varētu būt noderīga ikvienam interesentam, piemēram, dažādu pakalpojumu sniedzējiem, kuri pakalpojuma sniegšanai veic bērnu personas datu apstrādi vai sagatavo informatīvus materiālus bērniem, vai arī sniedz cita veida pakalpojumus, kuru mērķauditorija, iespējams, ir bērni.

Rekomendācija ir izstrādāta, ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 29. panta datu aizsardzības darba grupas apstiprināto viedokli Nr.1/2008 (WP 147) „Bērnu personas datu aizsardzība”⁵, kā arī, ņemot vērā Datu valsts inspekcijas un Eiropas Savienības dalībvalstu iestāžu, kuras uzrauga personas datu aizsardzību, pieredzi.

5 Dokumentu skatīt Eiropas Komisijas Tiesiskuma, brīvības un drošības ģenerāldirektorāta interneta mājas lapā: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-5.



Definīcijas

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

- pārzinis ir reģistrēts Latvijas Republikā;
- datu apstrāde tiek veikta ārpus Latvijas Republikas robežām teritorijās, kas pieder Latvijas Republikai saskaņā ar starptautiskajiem līgumiem;
- 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, ka personas dati netiek izpausti trešajām personām. Piemēram, elektroniskās piezīmju grāmatiņas, adrešu grāmatas, ģimenes foto albūmi, ģimeņu mājas lapas ar ierobežotu pieeju.

Gadījumā, kad personas dati (piemēram, fotogrāfijas) tiek ievietotas tiešsaistes sociālajā tīklā, iepriekš minētais izņēmums neattiecas, jo personas dati tiek nodoti trešām personām – sociālā tīkla portāla uzturētājam un lietotājiem).

Tāpat likums neattiecas uz juridisko personu datiem, piemēram, juridisko personu nosaukumiem, izņemot gadījumus, kad tie ietver fizisku personu vārdus.

Personas datu apstrāde – jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākša-

nu, reģistrēšanu, ievadišanu, 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, utt.

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, personas raksturojums, atzīmes. Ne vienmēr šāda informācija ir tieši saistīta ar personas vārdu, uzvārdu, bet gan var tikt saistīta ar personu, lai identificētu un uzzinātu personas paradumus. Sīkāk skatīt Datu valsts inspekcijas rekomendācijā „Personas datu definīcija”.

Datu subjekts – fiziska persona, kuru var tieši vai netieši identificēt un kuras personas dati tiek apstrādāti. Piemēram, skolēni, skolēnu vecāki, skolotāji.

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. Pārzinis, piemēram, var būt konkrēta pašvaldība, kā arī skola, ja tai kā juridiskai personai ir tiesībspēja un rīcībspēja.

Pārzinim ir pienākums nodrošināt personas datu aizsardzības principu ieviešanu, pēc pieprasījuma informēt personas par to pieejas tiesībām personas datiem, tiesībām tos labot, kā arī likumā noteiktos

gadījumos reģistrēt personas datu apstrādi 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 ārpakalpojumu 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 (attieciņi – gan skolēnu un viņu vecāku, gan skolotāju tiesības).

Informācijas aprites loma skolā ir svarīga bērnu tiesību aizsardzības nodrošināšanai, kā arī informācijas apmaiņa ar vecākiem ir būtiska izglītības procesa nodrošināšanai. Tādēļ svarīgi to īstenot, ievērojot personas datu aizsardzības prasības. Tomēr, personas datu aizsardzību nevajadzētu uzskatīt par šķērslī informācijas apmaiņai, bet gan par noteikumu ietvaru, lai tiktu nodota tāda informācija, kas nepieciešama konkrētajā situācijā konkrētiem indivīdiem (piemēram, ja to nosaka normatīvie akti).

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 šajā kontekstā svarīgs ir caurskatāmības un personu (skolēnu, darbinieku) uzticēšanās aspekts. Pārzinim ir jānodrošina, lai katram personas datu veidam būtu nepārprotams un skaidrs apstrādes mērķis, lai būtu skaidri noteikts, kādos gadījumos personas dati var tikt nodoti citām personām un iestādēm, kā arī jānodrošina, ka personas dati ir drošībā un aizsargāti.

Personas datu apstrādei ir jāatbilst šādiem personas datu apstrādes labās prakses principiem:

- Dati tiek apstrādāti godīgi un likumīgi.
- Datu apstrāde tiek veikta konkrētiem mērķiem un tikai saskaņā ar tiem.
- Dati ir adekvāti (ne pārmērīgi).
- Dati ir precīzi.
- Dati netiek glabāti ilgāk kā nepieciešams.
- Dati tiek apstrādāti saskaņā ar datu subjektu tiesībām.
- Dati ir drošībā.
- Dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas un adekvātas aizsardzības.

Personas datu apstrādes mērķa noteikšana

Personas datus var apstrādāt tikai likumīgam un iepriekš noteiktam mērķim, kas nepieciešams skolas funkciju izpildei. Skolas direktors vai pašvaldības

vadītājs (atkarībā no tā, vai pārzinis ir skola vai pašvaldība) atbild par šādu mērķu noteikšanu (izņemot, kad datu apstrādes mērķis noteikts ārējos 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

Drīkst apstrādāt tikai tādus personas datus, kas nepieciešami noteikta mērķa sasniegšanai. Piemēram, pieprasīt informāciju par skolēna vecāku ienākumiem nav atbilstoši, jo tas nav saistīts ar mērķa sasniegšanu – skolas 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

Pārzinim ir jānodrošina personas datu drošība skolā, 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, palīgpersonālam) ir nepieciešams piekļūt.

Ir jānodrošina, lai personas datus nebūtu iespējams sagrozīt, bojāt un lai tiem nepieklūtu nepilnvarotas personas. Piemēram, ārpakalpojumu sniedzēju gadījumos līgumos ir jānosaka to atbildība par datu drošību.

Pārzinim ir arī jānodrošina, lai tiktu 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 apstrādājamiem personas datu veidiem un to riskiem. Piemēram, jābūt augstam autentifikācijas (lietotāja identitātes pārbaude) līmenim attiecībā uz piekļūšanu testu (jeb pārbaudījumu, ieskaīšu, eksāmenu) rezultātiem, sensitīvus personas datus (t.i. personas datus, 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 arī informēt datu subjektu par iespējamiem personas datu saņēmējiem, par iespējām

un kārtību datu subjektam piekļūt saviem personas datiem, 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, skolēna vecāki, kas pārstāv skolēnu, skolotāji, skolas darbinieki) var pieprasīt jebkuru informāciju par sevi (datu subjektu), kas ir iestādes rīcībā (ja likums tieši neaizliedz to sniegt), kā arī viņam ir tiesības pieprasīt datus labot vai dzēst, ja tie ir nepilnīgi, novecojuši, nepatiesi, pretlikumīgi iegūti, vai arī vairs nav nepieciešami vākšanas mērķim. Turklāt datu subjektam ir tiesības saņemt informāciju par to, kurām trešajām

personām pārzinis ir nodevis datus par konkrēto datu subjektu.

Pārzinim ir pienākums sniegt atbildi datu subjektam uz tā informācijas pieprasījumu mēneša laikā no attiecīgā pieprasījuma saņemšanas dienas. Nesaņemot šādu informāciju, datu subjektam ir tiesības vērsties Datu valsts inspekcijā ar sūdzību.

Skolēnu datu izpaušana trešajām personām

Izpaužot skolēnu personas datus 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 tad nepieciešams saņemt rakstveida informācijas pieprasījumu, lai varētu identificēt informācijas pieprasītāju un izvērtēt, kādā apjomā informācija ir sniedzama. Neskaidrību gadījumā iespējams zvanīt Datu valsts inspekcijai vai nosūtīt elektroniskā pasta vēstuli uz e-pasta adresi info@dvi.gov.lv.

Ja speciālie normatīvie akti neparedz tiesības trešajām personām iegūt personas datus, bet trešā persona lūdz informāciju par skolēnu, tad varat jautāt vecākiem, vai viņi piekrīt, ka jūs izpaužat personas datus par skolēnu vai viņa 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. Iesakām skolām atrunāt

kārtību, saskaņojot ar vecākiem, kā par notikumiem skolā tiek informēti masu saziņas līdzekļi.

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

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

➤ 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, nosūtīt informāciju prokuratūrai.

➤ Inspekcija veic personas datu apstrādes pārbaudes uz vietas. Inspekcijai ir tiesības brīvi apmeklēt jebkuras nedzīvojamās telpas, kurās notiek personas datu apstrāde, 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 uzrādīt dokumentus un sniegt citu informāciju, kas attiecas uz pārbaudāmo personas datu apstrādi, kā arī pieprasīt jebkuras personas datu apstrādes iekārtas vai informācijas nesēja pārbaudi un noteikt ekspertīzi pārbaudāmo jautājumu izpētei.

➔ 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;
- ➔ personas koda apstrāde ir nepieciešama, lai sasniegtu noteiktu personas datu apstrādes mērķi;
- ➔ 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

Fotogrāfijas mūsdienās ir kļuvušas par neatņemamu ikdienas dzīves sastāvdaļu, turklāt tās tiek iegūtas, ne tikai fotografējot ar fotoaparātu, bet arī ar mobiliem telefoniem, viedtālruniem, planšetdatoriem un citām ierīcēm, kā arī tās tiek izmantotas, saglabājot fotoattēlus digitālā formātā un publicējot tos virtuālajā vidē.

Personas vai personu grupas fotogrāfiju izmantošana ir arī vispārēja prakse skolās. Piemēram, fotogrāfijas tiek izmantotas, pievienojot tās skolēnu dokumentiem, publicējot skolu informatīvajos materiālos, skolu avīzēs, interneta mājas lapās, vai izvietojot publiski skolas telpās. Informāciju tehnoloģijas piedāvā aizvien jaunas iespējas, taču tas nozīmē, ka gan pedagogiem, gan vecākiem, gan arī skolēniem ir jāapzinās riski, kas saistīti ar šīm iespējām, kā arī jābūt informētiem, kā aizsargāt savas tiesības un neaizskart citu personu tiesības uz privātumu gan attiecībā uz fotografēšanu, gan fotogrāfiju publiskošanu. Turklāt nepieciešams atcerēties, ka draudus nerada informāciju tehnoloģijas pašas par sevi, bet gan tas, kā indivīdi tās izmanto.

Tādēļ izglītošanas jautājums par dažādiem personas datu aizsardzības aspektiem ir ļoti būtisks.

Attiecībā uz katru konkrēto fotogrāfiju, kurā redzams kāds indivīds vai indivīdu grupa, ko ir iespējams iden-



tificēt, nepieciešams saņemt viņu atļauju šo fotogrāfiju publicēšanai. Tas attiecināms arī uz klases fotogrāfijām – nepieciešams saņemt vecāku piekrišanu, pirms tiek organizēta klases fotografēšana.

Kā arī skolai līgumā ar fotogrāfēšanas pakalpojumu sniedzēju nepieciešams atrunāt to, ka bērnu fotogrāfijas netiks izmantotas citam mērķim, kā tikai tam, kādēļ tās tiek uzņemtas.

Kāpēc jāaizsargā personas fotogrāfija?

Personas attēls ir uzskatāms par personības raksturīgu pazīmi, 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?

Ir jābūt vienošanās ar personu, kas tiek fotografēta. Piemēram, skola izstrādā iekšējo kārtību par fotografēšanu un/vai filmēšanu skolā, kur iekļauj arī 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 pasākumus 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 skolas intranetā, internetā, utt.).



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 lūgt skolēnu vecākiem atļauju viņu bērnu fotogrāfiju izvietojumam 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 uz žurnālistu izteiktu vēlmi skolā filmēt.

Pirms bērnu fotogrāfiju publiskošanas, ieteicams katram rast atbildes uz šādiem jautājumiem:

➤ Kāds ir iemesls konkrētās fotogrāfijas publikošanai? Ko ar konkrētās fotogrāfijas publikošanu ir mēģināts pateikt?

➤ Vai vēlamies, lai apskatīt fotogrāfiju, arī citas personas par to uzzina vai viņiem par to būtu nepieciešams uzzināt?

➤ Vai fotogrāfija ir uzskatāma par pozitīvu informāciju un vai to vēlēsimies redzēt publiski arī pēc 10 gadiem?

➤ Vai es vēlētos, lai šāda fotogrāfija tiktu publicēta arī par mani?

➤ Vai konkrētā fotogrāfija parāda skolu/ klasi/ bērnu pozitīvā gaisotnē?

➤ Ko teiktu konkrētais bērns, ieraugot publicētu savu fotoattēlu?

➤ Bērna draugu vai skolotāju fotogrāfijas var tikt publicētas (piemēram, ievietotas tiešsaistes sociālo tīklu portālos, publicētas blogos) tikai tad, ja persona, kura redzama fotogrāfijā, neiebilst.

Skolēnu datu apstrāde izmantojot internetu

Gandrīz katrai skolai ir izveidota interneta mājas lapa, kurā tiek atspoguļoti svarīgākie skolas dzīves notikumi, skolēnu sasniegumi un cita aktuālā informācija. Turklāt ikviens var ievietot skolā uzņemtu fotogrāfiju internetā, t.sk. tiešsaistes sociālajos tīklos.

Pastāv arī vairāki portāli vai sistēmas, kas nodrošina, ka skolēna datiem var piekļūt, izmantojot internetu, piemēram, portāls E-klase.

➤ Šajā 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 ir saistīti 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, utt. Tāpat sistēmas lietotājiem jābūt ziņojumiem par sistēmas konfidencialitātes jautājumiem.

➤ Nepieciešams informēt lietotājus par to tiesībām saskaņā ar Fizisko personu datu aizsardzības likumu. Informācijai par portāla drošu lietošanu ir jābūt pieejamai attiecīgajā pakalpojuma sniedzēja interneta mājas lapā, kā arī jābūt pieejamai tajā brīdī, 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 nodrošināts tās caurspīdīgums, informējot par to lietotājus. Ir skaidri jānosaka abu pušu (skolas un lietotāju) pienākumi, informējot par kontroles nosacījumiem un sankcijām pret lietotājiem, ja tie neievēro 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, lai katra skolēna novērtējums (arī dažādas piezīmes attiecībā uz skolēna mācību procesu) būtu pieejams tikai tiem skolas darbiniekiem, kuriem tas ir nepieciešams darba pienākumu

izpildei, un tikai pašam skolēnam vai viņa likumīgam pārstāvim (piemēram, vecākiem).

Statistikas dati un citi pētījumi

Lielākajā daļā gadījumu statistikas datu iegūšanai personas dati nav nepieciešami.

Pētījumos bieži tiek izmantoti dažādi skolēnu personas dati, kas iegūti no vairāk vai mazāk detalizētām aptaujas anketām. Šo datu (jo īpaši sensitīvo personas datu) vākšanai ir jāsaņem likumīgo pārstāvju atļauja, un 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, utt.) 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, kurā tiek apstrādāti biometrijas dati, vai arī attiecībā uz ierīci, kurā glabājas dati.

Ieviešot skolās biometrijas datu apstrādi, ir jāveic risku izvērtēšana, izvērtējot nepieciešamību izmantot personu biometrijas datus, lai sasniegtu paredzēto mērķi, utt. 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.

Pirms videonovērošanas kameru uzstādīšanas ir jāveic risku izvērtēšana, ņemot vērā dažādu iespējamo 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, un attiecīgi nav nepieciešams ieviest biometrijas datu apstrādi iekļūšanai skolā.

➔ Pirms videonovērošanas iekārtu uzstādīšanas pašvaldībai vai skolas administrācijai ir jāizvērtē:

- plānotie ieguvumi, uzstādot minētās ierīces – vai šie ieguvumi ir būtiskāki par iespējamo negatīvo efektu uz personām (skolēniem, viņu vecākiem, skolotājiem, u.c.);
- vai videonovērošanas ierīču izmantošana tiešām ir nepieciešama, un vai tā ir efektīva mērķa sasniegšanai;

- vai nepastāv citi efektīvi līdzekļi vai veidi paredzēto mērķu sasniegšanai, neizmantojot videonovērošanas ierīces (t.i., izmantojot labākas kvalitātes durvis, īpaši aizsargātus stiklus, dažādas slēdzeņu sistēmas un kustības detektorus vai citus sensorus īpašuma vai personu vitāli svarīgu interešu aizsardzībai, utt.);

- vai nepieciešams saglabāt ierakstus no videonovērošanas iekārtām, vai veikt videonovērošanu reālā laika režīmā;

- vai veikt ierakstus pastāvīgi, vai tikai, ja iestājas kāds noteikts kritērijs;

- vai ir iespējams sasniegt mērķi, veicot tikai noteiktas telpas daļas novērošanu;

- vai uzstādīt mobilu videonovērošanas ierīci vai pastāvīgi filmējošu;

- vai videonovērošanas ierīces filmēšanas perimetrs būs nemainīgs, vai tas automātiski mainīsies, vai to varēs mainīt manuāli;

- vai attēlu varēs palielināt, cik liela būs optikas izšķirtspēja, kas darīs iespējamu saskatīt sīkākās attēla detaļas, vai arī tiks iegūts daudz vispārīgāks attēls.

➔ **Proporcionalitātes princips.** Ja videonovērošanas ieviešana atbilst sasniedzamajiem drošības mērķiem (telpu piekļūšanas kontrole), tas vienlaicīgi nevar būt par pamatu, lai novērotu noteiktus darbiniekus vai noteiktas personu grupas, kuru novērošana nav nepieciešama drošības mērķiem. Videokameru skaits, izvietojums, novērošanas perimetrs, kameru funkcijas un kameru darbības periodiskums, vai novērojamo personu pienākumi ir visi tie faktori, kas



jāņem vērā, kad tiek novērtēta videonovērošanas proporcionalitāte.

Piemēram – iespējams, ka videonovērošanas sistēma būs nelikumīga, ja tā tiks 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.

Jebkura persona, kas tiek filmēta vai var tikt filmēta, ir skaidrā un saprotamā veidā jāinformē par videonovērošanu, piemēram, izvietojot brīdinājuma zīmes pie ieejas telpās vai teritorijā, tajās attiecīgi norādot, kas ir atbildīgs par videonovērošanas veikšanu un ar kādu mērķi videonovērošana tiek veikta.

• *Atbilstošu dokumentu izstrāde*

Ir vēlams iestādes dokumentos skaidri identificēt videonovērošanas mērķus un kārtību, 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.

• *Piekļuve 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 uzglabāšanas ilgums nevar pārsniegt dažas dienas un ieraksti ir jāiznīcina pēc šī perioda, izņemot gadījumus, ja tiek veikta izmeklēšana vai saņemts tiesībsardzības iestāžu rakstisks informācijas pieprasījums. Šim periodam jebkurā gadījumā nevajadzētu pārsniegt mēnesi.



- **Jāievēro noteiktas formalitātes pirms videonovērošanas ieviešanas**

Videonovērošana (ja tās rezultātā tiek saglabāti ieraksti) nevar tikt uzsākta pirms tās reģistrēšanas. Datu valsts inspekcijā, turklāt reģistrācija ir jāveic pārzinim, kas ne vienmēr ir pati skola.

Skolu mājas lapu veidošana internetā

Skolu interneta mājas lapas ir kļuvušas par daļu no skolas ikdienas dzīves. Tā kā mājas lapa ir izvietota internetā, tad tā ir pieejama publiski. Īpaši nepieciešams izvērtēt riskus, izveidojot interneta vai intraneta mājas lapas, izmantojot mākoņdatošanas pakalpojumus, jo pārzinis ir atbildīgs par visu veikto personas datu apstrādi, neskatoties uz to, kādas tehnoloģijas jeb rīki tiek izmantoti personas datu apstrādei, kā arī par šo tehnoloģiju vai rīku izvēli.

Informācijas meklētāju rīki kļūst aizvien efektīvāki, tādējādi palielinot risku aizskart personu privātumu. Izmantojot personas vārdu, ir iespēja izveidot personas „virtuālo” biogrāfiju, piemēram, iegūstot informāciju par skolēna dalību ārpus skolas 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, kuru rezultātā mājas lapā tiek izplatīta godu un cieņu aizskaroša vai rasistiska informācija.

Lai vāktu personas datus (piemēram, pieteiktos aktuālākās informācijas saņemšanai, kas tiek publicēta skolas interneta mājas lapā, 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)

Šajā gadījumā ar vārdu „blogs” tiek saprastas personu veidotas tīmekļa vietnes, kā žurnāls vai personisku interešu prezentācija (piemēram, par sportu, kultūru, ideju apmaiņu, u.c.).

Blogs nav vietne, kur persona var jebko izvietot/ publiskot, neievērojot likuma noteikumus. Ir jāievēro konkrēti 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 bez atļaujas izvieto 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.

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 izmantošanu, atstāj „pēdas”. Līdz ar to ir neiespējami pilnībā dzēst informāciju, jo nav iespējams zināt, kā rīcībā informācija ir nonākusi (piemēram, kura persona informāciju ir





saglabājusi savā datorā). Aplūkojot interneta mājas lapas, tiek saglabāta informācija, ko pieļauj lietotāja dators: tas atstāj lietotāja datora „pēdas”.

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

Līdz ar to internetā ir pieejams liels informācijas apjoms par personu paradumiem – personu politiskie uzskati, informācija par personu seksuālo dzīvi, informācija par personu attiecībām – ir pieejama blo-

gos. Internetā ir pieejami arī videorullīši, kur bieži ir ievietota informācija, personai to nezinot.

Tāpat bērni bieži ir arī 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, utt.

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 un internetu. 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. Praksē tas ir grūti, jo piemēram, 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 vairākus gadus pēc informācijas publiskošanas internetā.

Ņemot vērā minēto, ir 10 ieteikumi savu personas datu aizsardzībai internetā.

➤ Pirms publicējat, padomājiet!

➤ 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?

➤ Internetā pieejamās informācijas apjoms par jums, pirmkārt, ir atkarīgs no tā, cik daudz jūs pats to tur publicējat. Esot sociālajos tīklos, jābūt modram: sniedziet par sevi pēc iespējas mazāk informācijas vai tik maz, cik maz ir pieļaujams.

➤ Pirms sākat lietot noteiktu sociālo tīklu, iepazīstieties ar noteikumiem, kā varat ietekmēt savu profila informāciju. Kā arī noskaidrojiet, kurš ir konkrētais sociālā tīkla portāla uzturētājs, ar kuru varēsiet sazināties problēmjautājumos. 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.

➤ Kontrolējiet savas darbības blogā, dažādos forumos: *Facebook*, *Twitter* u.c.

➤ Npublicējiet fotogrāfijas. Piemēram, apdomājiet – ja jūs šodien dāri pieejamas savas fotogrāfijas saviem draugiem, kas notiks, ja rīt kāds no viņiem vairs nebūs jūsu draugs un izplatīs visiem jūsu fotogrāfijas.

➤ Npublicējiet internetā informāciju, kas var ietekmēt un aizskart citas personas. Nedariet citām personām to, ko nevēlaties, lai citas personas nodara jums.

➤ Regulāri pārbaudiet, kas par jums ir publicēts internetā. Piemēram, ierakstot savu vārdu meklēšanas ierīcēs, jūs varat uzzināt, 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.

➤ Ja iespējams, lietojiet pseidonīmus, kas jūs neidentificē.

➤ Nepadariet pieejamas savas paroles un neizvēlieties ļoti vienkāršas paroles (piemēram, dzimšanas datums vai ģimenes locekļu vārdi). Izvēlieties dažādas paroles dažādām mājas lapām. Atcerieties izslēgt datoru vai aizvērt savu profilu, kad vairs nestrādājat ar datoru.

Personas datu apstrādes reģistrācija Datu valsts inspekcijā

Skolām, veicot skolēnu (audzēkņu) un pedagogu personas datu (t.i., skolēnu lietas, sekmju žurnāli, pedagogu uzskaiti) apstrādi, saskaņā ar Izglītības likumu 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.



Kur iegūt vairāk informācijas?

Kā redzams no šajā rekomendācijā aprakstītajām tēmām, personas datu aizsardzība skolās var būt sarežģīts uzdevums, kam nepieciešams gan laiks, gan finanšu līdzekļi, gan speciālista padoms. Bet šie pasākumi ir ļoti būtiski, lai jūs veiktu personas datu apstrādi atbilstoši normatīvo aktu prasībām.

Šajā rekomendācijā nav precīzu ieteikumu un gatavu atbilžu, jo katra organizācija personas datu apstrādi veic atšķirīgi, un tādējādi iespējamās situācijas arī ir atšķirīgas.

Datu valsts inspekcija (www.dvi.gov.lv)

Inspekcija sniedz konsultācijas personas datu aizsardzības jautājumos. Vairāk varat uzzināt Inspekcijas mājaslapā. Turpat atradīsiet arī informatīvus materiālus, rekomendācijas un skaidrojumus par datu aizsardzības un drošības tēmām, kā arī normatīvos aktus – Fizisko personu datu aizsardzības likumu un uz tā pamata izdotos Ministru kabineta noteikumus.

Iesakām iepazīties ar šādām rekomendācijām:

- Personas datu definīcija;
- Personas datu aizsardzība darba vietās;
- Personas datu apstrādes drošība;

➤ Personas datu apstrāde tiešsaistes sociālajos tīklos;

➤ Datu apstrāde videonovērošanas jomā.

Esi drošs (www.esidross.lv)

Šī mājaslapa ir paredzēta ikvienam, kas rūpējas par sava datora drošību un savu drošību internetā. Mājas lapu uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tajā informācijas tehnoloģiju speciālisti no Drošības ekspertu grupas sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz jautājumiem par jūsu datora drošību un jūsu drošību internetā.

Drošs internets (www.drossinternets.lv)

Informācijas resurss, par kura saturu atbild Latvijas Interneta asociācija. Šeit varat atrast gan ieteikumus bērniem, jauniešiem un pieaugušajiem interneta drošai lietošanai, gan arī nozares pētījumus un aptaujas.

Bērnu tiesību aizsardzība (www.bti.gov.lv)

Valsts bērnu tiesību aizsardzības inspekcija uzrauga un kontrolē normatīvo aktu ievērošanu bērnu tiesību aizsardzības jomā. Šīs institūcijas interneta mājas lapā pieejama informācija par dažādiem bērnu tiesību aizsardzības aspektiem, tajā skaitā arī e-konsultācijas bērniem un jauniešiem.

Datu valsts inspekcija

Tālr. 67223131
Blaumaņa iela 11/13-15,
Rīga, LV-1011
e-pasta adrese: info@dvi.gov.lv
www.dvi.gov.lv

Telefonkonsultācijas

katru darba dienu laika posmā no plkst. 13:00-15:00
tālrunis 67223131

