LATVIJAS REPUBLIKAS KULTŪRAS MINISTRIJA

S T A Ņ I S L A V A B R O K A
D A U G A V P I L S M Ū Z I K A S V I D U S S K O L A

Reģ. Nr. 90000066001
Kandavas ielā 2A, Daugavpilī, LV-5401
Tālrunis: 65407900, e-pasts: sbdmv@sbdmv.lv

IEKŠĒJIE NOTEIKUMI

Daugavpilī

21.05.2018. Nr.1-4/8

PERSONU DATU APSTRĀDES AIZSARDZĪBAS IEKŠĒJIE NOTEIKUMI STAŅISLAVA BROKA DAUGAVPILS MŪZIKAS VIDUSSKOLĀ

Izdoti saskaņā ar Ministru kabineta
2001.gada 30.janvāra noteikumu Nr.40
„Personas datu aizsardzības obligātās tehniskās
un organizatoriskās prasības" 5.punktu

1. Vispārīgie jautājumi

1. Staņislava Broka Daugavpils Mūzikas vidusskolas (turpmāk – Skola) personas datu apstrādes aizsardzības iekšējie noteikumi (turpmāk – noteikumi) nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot Skolas informācijas resursu un informācijas sistēmu drošību.

2. Noteikumu mērķis ir noteikt skolas organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu tikai paredzētajiem mērķiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību.

3. Saskaņā ar Fizisko personu datu aizsardzības likumu uz fizisko personu datu apstrādi ir attiecināmi šādi termini:

3.1. datu subjekts — fiziska persona, kuru var tieši vai netieši identificēt;

3.2. datu subjekta piekrišana — datu subjekta (nepilngadīgas personas likumiskā pārstāvja) brīvi, nepārprotami izteikts gribas apliecinājums, ar kuru viņš atļauj apstrādāt savus personas datus atbilstoši pārziņa sniegtajai informācijai;

3.3. personas dati — jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisku personu;

3.4. personas datu apstrāde — jebkuras ar fiziskas personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu;

3.5. personas datu apstrādes sistēma — jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus;

3.6. personas datu operators — pārziņa pilnvarota persona, kas veic personas datu apstrādi pārziņa uzdevumā;

3.7. personas datu saņēmējs — fiziskā vai juridiskā persona, kurai tiek izpausti fiziskas personas dati;

3.8. sensitīvi personas dati — 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;

3.9. pārzinis — Skola, kas nosaka personas datu apstrādes mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar normatīvajiem aktiem par fizisko personu datu aizsardzību;

3.10. trešā persona — jebkura fiziskā vai juridiskā persona, izņemot datu subjektu (likumisko pārstāvi), Skolu vai personas, kuras tieši pilnvarojusi Skola.

4. Personas datu apstrāde tiek veikta Skolas telpās.

5. Noteikumi ir saistoši visām personas datu apstrādē iesaistītajām personām.

6. Noteikumi attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.

7. Par personu datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild Skolas direktors, kurš pats vai ar norīkoto personu starpniecību kontrolē personu datu apstrādes sistēmu drošību (turpmāk – pārzinis).

8. Pārzinis var bez brīdinājuma dzēst vai mainīt pilnvarotās personas datus personas datu apstrādes sistēmas piekļuvei, ja pilnvarotā persona pārkāpj šos iekšējos normatīvos aktus, kā arī citus ārējos normatīvos aktus un ētikas normas.

9. Pārzinis ir tiesīgs pieprasīt no pilnvarotās personas rakstveida apliecinājumu par šo noteikumu un konfidencialitātes prasību ievērošanu darbā ar personas datiem un personas datu apstrādes sistēmu, kā arī veikt visas citas darbības, kuras uzskata par nepieciešamām, lai tiktu ievērotas visas normatīvo aktu prasības personu datu aizsardzības jomā.

10. Pārziņa pienākums ir rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot pilnvaroto personu drošu piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem no sistēmas.

2. Personas datu apstrādes sistēmas nodrošinājums

11. Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret fiziskās iedarbības radītu personas datu apdraudējumu un aizsardzību, kuru realizē ar programmatūras līdzekļiem.

12. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam Skolas darbinieku lokam. Datorizētas informācijas sistēmas (turpmāk – informācijas sistēma) datus drīkst izmantot tikai Skolas darbinieks, kuram pārzinis ir devis atļauju ar attiecīgiem piekļuves datiem (turpmāk – pilnvarotā persona).

13. Personas datu apstrādes sistēmas datortehnikas un programmatūras tehnisko uzstādīšanu un tās administrēšanu nodrošina persona, ar kuru Skola ir noslēgusi ārpakalpojuma līgumu vai arī šie amata pienākumi ietilpst attiecīga Skolas darbinieka darba pienākumos, kas konkretizēti amata aprakstā vai darba devēja rīkojumā.

14. Informācijas sistēmas aizsardzība tiek nodrošināta ar lietotājvārdu un paroli, kurai jābūt komplicētai, izmantojot burtu, ciparu un rakstzīmju kombināciju un kura ir zināma tikai pilnvarotajai personai (ne mazāk kā 8 simboli).

15. Apstrādājot personas datus informācijas sistēmā, tiek nodrošināta tikai pilnvarotu personu piekļūšana pie tehniskajiem līdzekļiem un dokumentiem.

16.Pārzinis personas datu saturošas programmatūras apstrādei lieto šādas ierīces:

16.1. portatīvo vai personālo datoru ar operētājsistēmu;

16.2. citas licencētas iekārtas un programmatūru pēc vajadzības.

17. Informācijas sistēmas personas datu apstrādes loģisko drošību nodrošina uzstādītā satura vadības sistēma, kas neļauj personas datus labot vai dzēst bez sankcionētas pieejas. Pieeja datu rediģēšanai pieejama tikai pārzinim un viņa pilnvarotajām personām.

3. Personu datu apstrādes organizatoriskā procedūra, aizsardzība pret ārkārtējiem apstākļiem un datu drošības pasākumi

18. Personas datu apstrāde Skolā ir atļauta atbilstoši normatīvajos aktos noteiktajam un tikai tad, ja ir vismaz viens no šādiem nosacījumiem:

18.1. saņemta personas datu subjekta piekrišana;

18.2. datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;

18.3. datu apstrāde nepieciešama Skolai likumā noteikto pienākumu veikšanai;

18.4. datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;

18.5. datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti Skolai;

18.6. datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu Skolas vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.

19. Pārzinis nodrošina tehnisko resursu fizisku aizsardzību pret ārkārtas apstākļiem (ugunsgrēks, plūdi un citi ārkārtas apstākļi). Pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar ugunsdrošības noteikumiem Skolā, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.

20. Lai izvairītos no tehnisko resursu tīšas bojāšanas radītām sekām pārzinis veic šādas darbības:

20.1. reizi mēnesī izveido informācijas sistēmas (to skaitā datubāzes) rezerves kopijas;

20.2. reizi mēnesī veic informācijas sistēmas satura vadības sistēmas vispārīgu apskati.

20.3. reizi 6 (sešos) mēnešos atjaunina vai uzlabo informācijas sistēmas satura vadības sistēmu, ja tas ir iespējams un nepieciešams.

21. Informācijas sistēmas glabāšanas kārtību nosaka Skolas direktors.

22. Informācijas sistēmas slēgšanas gadījumā Skolas direktors vai viņa pilnvarota atbildīgā persona dzēš informācijas sistēmu un satura vadības sistēmas saturu, datubāzu saturu, kā arī visas citas saistītās datnes.

23. Ja nepieciešams dzēst datus no informācijas sistēmas, pārzinis nodrošina pilnīgu datu dzēšanu no informācijas sistēmas.

4. Pilnvarotās personas paroles garums un uzbūves nosacījumi

4.1. Paroles uzbūve un pilnvarotās personas atbildība

24. Minimālais pilnvarotās personas paroles garums informācijas sistēmas vietnē ir 8 simboli.

25. Pilnvarotās personas parole var sastāvēt no datorrakstā pieejamajiem simboliem.

26. Pārzinis neatbild par problēmām ar paroles ievadīšanu, ja pilnvarotās personas parole satur mīkstinājuma zīmes un garumzīmes.

27. Par paroles drošību un sarežģītību atbild pilnvarotā persona.

4.2. Paroles lietošana

28. Pilnvarotā persona lieto savu kontu informācijas sistēmā, izmantojot pilnvarotās personas vārdu un paroli, ko iegūst reģistrācijas ceļā.

29. Pilnvarotā persona iegaumē savu paroli un neizpauž citām to personām.

30. Pilnvarotā persona nomaina paroli ne retāk kā 1 reizi pusgadā.

4.3. Paroles drošība

31. Ja pilnvarotās personas paroli uzzina trešā persona, pilnvarotās personas nekavējoties nomaina esošo paroli uz jaunu, ievērojot šo noteikumu prasības.

32. Ja pilnvarotajai personai ir aizdomas, ka trešā persona piekļūst pilnvarotās personas kontam, pilnvarotā persona nekavējoties par to informē pārzini.

5. Pilnvarotās personas tiesības, pienākumi un atbildība

33. Pilnvarotajai personai ir tiesības izmantot tikai darba vajadzībām viņam lietošanā nodotos datorus un to programmatūru.

34. Pilnvarotā persona nedrīkst izpaust ziņas par Skolas datoru tīklu uzbūvi un konfigurāciju, kā arī atklāt ierobežotas pieejamības informāciju nepilnvarotām personām. Personas datus var izpaust, pamatojoties uz rakstveida iesniegumu vai vienošanos, norādot datu izmantošanas mērķi, ja likumā nav noteikts citādi. Personas datu pieprasījumā norādāma informācija, kas ļauj identificēt datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjoms. Jebkura informācijas sniegšana iepriekš saskaņojama ar Skolas direktoru.

35. Pilnvarotā persona nedrīkst atļaut piekļūt personas datiem nepiederošām personām, ja tie nav nepieciešami tiešo darba pienākumu pildīšanai.

36. Pilnvarotās personas pienākums ir saglabāt un bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību izbeigšanas.

37. Pilnvarotās personas pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to nelikumīgu apstrādi.

38. Pilnvarotā persona ir atbildīga par datortehniku, kas nodota viņa rīcībā, kā arī par dokumentiem, kas nepieciešami viņa darba pienākumu pildīšanai.

39. Pilnvarotajai personai ir aizliegts izmantot nelicencētu programmatūru.

40. Aizliegta jebkāda nešifrēta bezvadu datortīkla izmantošana Skolā (Unencrypted Wireless Networks).

41. Pilnvarotā persona nedrīkst izdarīt darbības, kas būtu vērstas pret informācijas sistēmas drošību, izmantojot neparedzētas pieslēgšanās iespējas.

42. Beidzot (pārtraucot) darbu ar informācijas sistēmu, pilnvarotā persona aizver pārlūkprogrammu.

43. Pilnvarotā persona nedrīkst saņemto informāciju pārveidot, piedalīties tās pārdošanā vai cita veida atsavināšanā, reproducējot kopumā vai tās daļas, izmantot to citu datu apstrādes sistēmu izveidei, kā arī glabāt publiski pieejamās vietās.

44. Ja ir aizdomas par tīšiem bojājumiem, kas ir radušies informācijas sistēmai paroles publiskošanas rezultātā vai citu iemeslu dēļ, pilnvarotā persona par to nekavējoties ziņo Skolas vadībai.

45. Par pilnvarotās personas prettiesisku nodarījumu tiek piemērota normatīvajos aktos noteiktā atbildība.

Direktors A.Broks