Ķeguma novada dome
ĶEGUMA KOMERCNOVIRZIENA VIDUSSKOLA
Reģ.Nr.4313900201
Skolas ielā 10, Ķegumā, Ķeguma novadā, LV 5020
Tālrunis- fakss 65055275, e-pasts kegumaskola@inbox.lv

ĶEGUMĀ

APSTIPRINU
Ķeguma novada domes priekšsēdētājs
_____ R.OZOLS
2012.gada _____

2012.gada 2.aprīlī Nr. KVS/1-59/12/65

Personu datu apstrādes aizsardzības iekšējie noteikumi

Izdoti saskaņā ar Ministru kabineta 2001.gada 30.janvāra noteikumu Nr.40 „Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" 5.punktu un Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 1.punktu

I. Vispārīgie jautājumi

1. Ķeguma komercnovirziena vidusskolas (turpmāk – izglītības iestāde) personas datu apstrādes aizsardzības iekšējie noteikumi (turpmāk – noteikumi) nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot izglītības iestādes informācijas resursu un informācijas sistēmu drošību.

2. Noteikumu mērķis ir noteikt izglītības iestādes 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 (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 — fiziskas personas dati, kas norāda personas rasi, etnisko izcelsmi, kā arī sniedz informāciju par personas veselību;

3.9. pārzinis — izglītības iestāde, 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), izglītības iestādi vai personas, kuras tieši pilnvarojusi izglītības iestāde.

4. Personas datu apstrāde tiek veikta izglītības iestādes telpās.

5. Noteikumi ir saistoši visiem personas datu apstrādes lietotājiem.

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 izglītības iestādes vadītājs, kurš pats vai ar norīkoto personu starpniecību kontrolē personu datu apstrādes sistēmu drošību (turpmāk – pārzinis).

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

9. Pārzinis ir tiesīgs pieprasīt no lietotāja 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 nepieciešamu, lai tiktu ievērotas visas normatīvo aktu prasības personu datu aizsardzības jomā.

10. Pārziņa pienākums ir rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot lietotāju piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem sistēmā.

II. 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 izglītības iestādes darbinieku lokam. Informācijas sistēmas datus drīkst izmantot tikai izglītības iestādes darbinieks, kuram pārzinis ir devis atļauju ar attiecīgiem piekļuves datiem (turpmāk – lietotājs).

13. Personas datu apstrādes sistēmas datortehnikas un programmatūras tehnisko uzstādīšanu un to administrēšanu nodrošina persona, ar kuru izglītības iestāde vai pašvaldība ir noslēgusi atsevišķu līgumu.

14. Datorizētās informācijas sistēmas (turpmāk – informācijas sistēma) aizsardzība tiek nodrošināta ar lietotājvārdu un paroli, kurai jābūt komplicētai, izmantojot burtu, ciparu un rakstzīmju kombināciju un kura ir zināma tikai lietotājam (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 konkrētajam personas datu subjektam un pārzinim.

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

18. Personas datu apstrāde izglītības iestādē 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 izglītības iestādei 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 izglītības iestādei;

18.6. datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu izglītības iestādes 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 izglītības iestādē, 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 6 (sešos) mēnešos 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 izglītības iestādes vadītājs.

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

23. Ja lietotājs vēlas dzēst savu lietotāja datus un lietotāja kontu, lietotājs nodrošina lietotāja datu pilnīgu dzēšanu no informācijas sistēmas.

IV. Lietotāja paroles garums un uzbūves nosacījumi

4.1. Paroles uzbūve un lietotāja atbildība

24. Minimālais lietotāja paroles garums informācijas sistēmas vietnē ir 8 simboli.

25. Lietotāja parole var sastāvēt no datorrakstā pieejamajiem simboliem.

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

27. Par paroles drošību un sarežģītību atbild lietotājs.

4.2. Paroles lietošana

28. Lietotājs lieto savu lietotāja kontu informācijas sistēmā, izmantojot lietotāja vārdu un paroli, ko iegūst reģistrācijas ceļā.

29. Lietotājs iegaumē savu paroli un neizpauž citām to personām.

30. Lietotājs nomaina paroli ne retāk kā 1 reizi pusgadā.

4.3. Paroles drošība

31. Ja lietotāja paroli uzzina trešā persona, lietotājs nekavējoties nomaina tagadējo paroli uz jaunu, ievērojot šo noteikumu prasības.

32. Ja lietotājam ir aizdomas, ka trešā persona piekļūst lietotāja kontam, lietotājs nekavējoties par to informē pārzini.

V. Lietotāja tiesības, pienākumi un atbildība

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

34. Lietotājs nedrīkst izpaust ziņas par izglītības iestādes 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 izglītības iestādes vadītāju.

35. Lietotājs nedrīkst atļaut piekļūt personas datiem nepiederošām personām, ja to nevajag tiešo darba pienākumu pildīšanai.

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

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

38. Lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī par dokumentiem, kas nepieciešami viņa darba pienākumu pildīšanai.

39. Lietotājam aizliegts izmantot nelicencētu programmatūru.

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

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

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

43. Lietotājs 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, lietotājs par to nekavējoties ziņo izglītības iestādes vadībai.

45. Par lietotāja prettiesisku nodarījumu tiek piemērota normatīvajos aktos noteiktā atbildība.

DIREKTORS E.VIŅĶIS