SIGULDAS NOVADA PAŠVALDĪBA

Siguldas Mākslu skola „Baltais Flīģelis"
Reģ.Nr. 4374902437
PVN Reģ.Nr.90000048152
Šveices ielā 19, Siguldā, LV – 2150x
e-pasts skola@baltaisfligelis.lv, www.baltaisfligelis.lv

IEKŠĒJIE NOTEIKUMI

Siguldā

2018.gada 17.maijā Nr.27

DATU AIZSARDZĪBAS NOTEIKUMI

Izdoti saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2.punktu

I. Vispārīgie jautājumi

1. Šie noteikumi nosaka pārziņa – Siguldas novada pašvaldības (turpmāk – pašvaldība) iestādes - Siguldas Mākslu skolas "Baltais Flīģelis" (turpmāk - iestāde) personas datu aizsardzības kārtību.
2. Noteikumu mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību, attiecībā uz fiziskās personas datu apstrādi pašvaldībā un tās iestādēs.
3. Personas datu apstrādes principi:

3.1. dati tiek apstrādāti likumīgi un godprātīgi;
3.2.datu apstrāde tiek veikta noteiktiem datu apstrādes mērķiem un tikai saskaņā ar tiem;
3.3.datu apjoms ir adekvāts un atbilstošs datu apstrādes mērķim;
3.4.dati ir precīzi un tiek atjaunoti;
3.5.dati netiek glabāti ilgāk nekā nepieciešams;
3.6.dati tiek apstrādāti, ievērojot datu subjekta tiesības;
3.7.dati ir drošībā (nav pieejami nepilnvarotām trešajām personām);
3.8.dati netiek pārsūtīti ārpus ES/EEZ (Eiropas Savienība / Eiropas ekonomiskā zona) bez adekvātas aizsardzības.

II. Personas datu apstrāde

4. Šie noteikumi attiecas uz iestādes veikto personas datu apstrādi – jebkuru darbību, kura tiek veikta ar jebkādu informāciju, kura attiecas uz identificētu vai identificējamu fizisku personu. Iestādes personas datu apstrāde tiek veikta elektroniski, izmantojot datorus, programmatūru, internetu utt., kā arī manuāli, reģistrējot dokumentus un iekārtojot, glabājot personas datu apstrādes lietas.
5. Iestādes veikto personas datu apstrādi reģistrē pārziņa pašvaldības personas datu apstrādes darbību reģistrā. Personas datu apstrādes darbību reģistru ar rīkojumu apstiprina pašvaldības izpilddirektore.
6. Iestādē tiek apstrādāti tikai tādi personas dati, kas ir atbilstoši Personas datu apstrādes reģistrā noteiktajiem mērķiem un noteiktajam datu apjomam.

7. Jaunu, Personas datu apstrādes darbību reģistrā neuzskaitītu personas datu apstrādes mērķu ieviešana ir jāsaskaņo ar pašvaldības Datu un informācijas drošības vadītāju (turpmāk – DID vadītājs).
8. iestādes darbinieki un amatpersonas (turpmāk – darbinieki) veic personas datu apstrādi darba līgumos, amatu aprakstos, rīkojumos, kā arī ārējos un iekšējos normatīvajos aktos noteikto pilnvaru ietvaros.

III. Par informācijas resursiem, tehniskajiem resursiem un personas datu aizsardzību atbildīgās personas un to pienākumi

9. Par informācijas resursu uzturēšanu iestādē (programmatūru, paroļu piešķiršanu un veidošanu, datu kopiju veidošanu u.c.) ir atbildīgi pašvaldības datortīkla administratori vai iestādes IT speciālists, jā tāda štata vienība ir izveidota.
10. Datortīkla administratori vai iestādes IT speciālists nodrošina:
    3.2.1. loģiskās aizsardzības pasākumus (paroles, antivīrusi, ugunsmūris, datu kopijas u.c.);
    3.2.2. informācijas resursu darbības atjaunošanu, ja noticis tehnisko resursu bojājums vai arī informācijas resursa darbība ir tikusi traucēta citu iemeslu dēļ.

11. Par tehniskajiem resursiem (datortehnikas, serveru u.c., uzturēšanu) ir atbildīgi pašvaldības datortīkla administratori vai iestādes IT speciālists .
12. Datortīkla administratori vai iestādes IT speciālists nodrošina:
    13.1.tehnisko resursu darbspēju;
    13.2.tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.
14. Personas datu aizsardzības organizēšanu, pārraudzību un kontroli iestādē veic DID vadītājs.
16. Par personas datu apstrādes atbilstību pašvaldības vai iestādes izdoto rīkojumu, šo noteikumu un citu normatīvo aktu prasībām pašvaldības iestādē ir atbildīgs iestādes vadītājs.
17. Iestādes vadītājs ar rīkojumu nosaka atbildīgās personas par datu apstrādi un to pienākumus iestādē.

III. Informācijas klasifikācija

18. Informācijas klasifikācijas līmeņi:
18.1. ierobežotas pieejamības informācija - ir tāda informācija, kura ir paredzēta ierobežotam personu lokam sakarā ar darba vai dienesta pienākumu veikšanu un kuras izpaušana vai nozaudēšana šīs informācijas rakstura un satura dēļ apgrūtina vai var apgrūtināt iestādes darbību, nodara vai var nodarīt kaitējumu personu likumiskajām interesēm;
18.2. vispārpieejamā informācija - ir tāda informācija, kas nav klasificēta kā ierobežotas pieejamības informācija.
19. Personas dati ir klasificējami kā ierobežotas pieejamības informācija, kurai ir tiesības piekļūt un veikt to apstrādi tikai pilnvarotiem darbiniekiem.
20. Iestāde ievieš papildu datu aizsardzības procedūras īpašas kategorijas personas datiem - personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētisko dati, biometriskie dati (veicot personas unikālu identifikāciju), veselības dati, dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju. iestāde izvērtē nepieciešamību ieviest papildu datu aizsardzības procedūras citiem datu veidiem (piem., datiem par sodāmību).
21. Katrai personas datu apstrādei, vadoties pēc aktuālās datu apstrādes risku analīzes rezultātiem, tiek noteikti atbilstoši drošības un aizsardzības pasākumi.

IV. Tehniskie resursi, ar kādiem tiek nodrošināta personas datu apstrāde

22. Iestāde personas datu apstrādei lieto šādus tehniskos resursus:
22.1. darbstacijas ar operētājsistēmu;
22.2. serverus ar operētājsistēmu;
22.3. pēc vajadzības citas iekārtas un tehniskos resursus.
23. tehniskos resursus, kurus izmanto attiecīgā personas datu apstrādē, uzskaita un kontrolē tehnisko resursu turētājs – Informācijas tehnoloģiju nodaļa.
24. visi tehniskie resursi tiek uzskaitīti grāmatvedības reģistrā kā pamatlīdzekļi.

V. Personas datu apstrāde elektroniskajā vidē

25. Personas datu apstrādes tehniskās un organizatoriskās prasības elektroniskajā vidē nosaka Siguldas novada pašvaldības domes informācijas sistēmu drošības politika un Informācijas sistēmu izmantošanas noteikumi.
26. Darbinieka vispārīgie pienākumi ir:
26.1. veikt datu apstrādi, ja tai ir tiesisks pamats;
26.2. veikt datu apstrādi Datu apstrādes reģistrā noteiktajiem mērķiem un tam nepieciešamajā apjomā;
26.3. nodrošināt personas datu pareizību un to savlaicīgu atjaunošanu, labošanu un dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi;
26.4. attiecībā uz elektroniskajiem dokumentiem ievērot lietvedības un arhīvniecības prasības attiecībā uz dokumentu apriti;
26.5. informācijas sistēmām lietot paroles, kas sastāv ne mazāk kā no 9 simboliem;
26.6. pēc darba vietas atstāšanas nodrošināt, ka telpas kurā glabājas dators vai ārējais datu nesējs tiek slēgtas. Ja datorus vai ārējos datu nesējus paredzēts lietot ārpus pašvaldības vai tās iestāžu telpām, nodrošināt, ka tiem nepiekļūst nepilnvarotas trešās personas.

VI. Manuālā personas datu apstrāde

27. Manuālā personas datu apstrāde (papīra formātā) tiek veikta atbilstoši datu aizsardzību regulējošo normatīvo aktu, kā arī normatīvo aktu par lietvedību un arhīvniecību prasībām.
28. Darbiniekiem ir pienākums:
28.1. veikt datu apstrādi, ja tai ir tiesisks pamats;
28.2. veikt datu apstrādi Datu apstrādes reģistrā noteiktajiem mērķiem un tam nepieciešamajā apjomā;
28.3. nodrošināt personas datu pareizību un to savlaicīgu atjaunošanu, labošanu un dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi;
28.4. ievērot lietvedības un arhīvniecības prasības attiecībā uz dokumentu apriti;
28.5. nodrošināt, ka dokumenti un tajos esošā informācija, kura satur personas datus bez tiesiska pamata nekļūst pieejama nepilnvarotām trešajām personām.
28.6. pēc darba vietas atstāšanas nodrošināt, ka telpas kurās glabājas personas datus saturoši dokumenti, tiek slēgtas.
28.7. gatavojot līguma projektus ar personas datu apstrādātājiem, nodrošināt, ka tajā tiek iekļautas normatīvajos aktos paredzētās personas datu aizsardzības atrunas.

VII. Pasākumi, kas veicami tehnisko resursu aizsardzībai pret ārkārtas apstākļiem

29. Iestāde iespēju robežās nodrošina tehnisko resursu aizsardzību pret dabas stihijām, ugunsgrēka, plūdiem u.tml.

30. Par ārkārtas apstākļu iestāšanos iestādē darbiniekiem pa tālruni ir jāziņo pašvaldības Informācijas tehnoloģiju nodaļas vadītājam (turpmāk – IT vadītājam), iestādes vadītājam un/ vai Darba un civilās aizsardzības speciālistam.
31. Noteikumu 30. punktā minētās personas pieņem lēmumu par tālāko rīcību ar tehniskajiem resursiem un ārkārtas apstākļu novēršanai piemērojamiem pasākumiem.

VIII. Informācijas nesēju glabāšanas un iznīcināšanas kārtība

33. Pirms tehnisko resursu (cietie diski, zibatmiņas, CD utt.) nodošanas utilizēšanai, personas dati no tiem dzēšami vai tehniskais resurss fiziski sabojājams tādā veidā, ka personas datus nav iespējams atjaunot, bet papīra dokumenti iznīcināmi papīra griezējā. Tehnisko resursu utilizēšanu veic pašvaldības IT nodaļas darbinieki.
34. Trešajām personām utilizācijai tehniskos resursus vai papīra dokumentus, ja tie satur personas datus, drīkst nodot, tikai ja rakstveida līgumā ir ietvertas konfidencialitātes prasības un iestādei ir tiesības un iespēja pārliecināties par to ievērošanu.
35. Par tehnisko un papīra dokumentu iznīcināšanu tiek sagatavots un parakstīts iznīcināšanas akts, kurā tiek fiksēti kādi tehniskie resursi, dokumenti, kad un kādā veidā ir iznīcināti.

IX. Datu subjekta tiesību realizācija

36. Datu subjektam ir tiesības:
36.1. iegūt informāciju par tās personas datu apstrādi iestādē.
36.2.iegūt informāciju par fiziskām vai juridiskām personām, kam noteikumu 36.1.punktā minētā informācija noteiktā laika posmā ir izsniegta par datu subjektu, izņemot normatīvajos aktos paredzētos gadījumus.
36.3. pieprasīt datu labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu. Tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību.
37. Lai realizētu kādu no noteikumu 36.punktā minētajām tiesībām, datu subjekts iesniedz Siguldas novada pašvaldībai vai iestādei iesniegumu. Ja iesniegumu saņem iestāde, tā to nosūta pašvaldībai.
38. Pašvaldība to izskata un atbildi sniedz viena mēneša laikā.
38. Ja ir objektīvs iemesls (piem., pieprasīto datu apjoms, nepieciešamība pieprasīt papildu informāciju, u.c.), pašvaldība vai iestāde var nosūtīt datu subjektam starpatbildi un pagarināt iesnieguma izsktīšanas termiņu līdz diviem mēnešiem.
39. Pašvaldība var atteikties izpildīt datu subjekta informācijas pieprasījumu vai tā izpildes nosacījumus, ja informācijas pieprasījums ir acīmredzami nepamatots vai pārmērīgs, jo īpaši to atkārtošanās dēļ.
40. Pašvaldība vai tās iestāde var uzaicināt datu subjektu pārzinim un datu subjektam abpusēji pieņemamā laikā iepazīties ar pieprasīto informāciju iestādē, ja informācijas pieprasījums ir nesamērīgi apjomīgs vai informācijas izsniegšana ārpus iestādes nav iespējama informācijas uzglabāšanas nosacījumu dēļ.

X. Personas datu apstrādes aizsardzības pārkāpumi

41. Par personas datu aizsardzības pārkāpumu (piem. dati nonākuši nepilnvarotu trešo personu rīcībā, citu šo noteikumu pārkāpumu) darbiniekiem ir pienākums nekavējoties ziņot DID vadītājam.
42.DID vadītājs izvērtē saņemto informāciju un nepieciešamības gadījumā konsultējoties ar IT vadītāju pieņem lēmumu par turpmāko rīcību.
43. Normatīvajos aktos paredzētos gadījumos DID vadītājs par personas datu aizsardzības pārkāpumu sniedz informāciju Datu valsts inspekcijai.
44.DID vadītājs veic personas datu aizsardzības pārkāpumu uzskaiti.

XI. Darbinieku tiesības, pienākumi, ierobežojumi un atbildība

45. Darbiniekiem ir šādi pienākumi:
45.1.pieprasīt piekļuvi informācijas resursiem, kas nepieciešami darba pienākumu pildīšanai;
45.2.datu apstrādes drošības incidentu gadījumā darbiniekam savu iespēju un pilnvaru robežās nodrošināt tehnisko un informācijas resursu drošību līdz datortīkla administratora vai iestādes IT speciālista ierašanās brīdim;
45.3.veikt visus nepieciešamos aizsardzības pasākumus, lai tam pieejamiem personas datiem nepiekļūtu trešās personas;
45.4.pamatot darba devējam nepieciešamību piekļūt vai veikto piekļuvi personas datiem un savas darbības kā informācijas sistēmā tā manuālā apstrādē;
45.5.sniegt palīdzību informācijas datu apstrādes drošības incidentu izmeklēšanā;
45.6.ievērto konfidencialitāti un neizpaust personas datus arī pēc darba attiecību izbeigšanās;
45.7.noteikumu 25. un 26., 27., 28. punktā minētie pienākumi.

46. Darbiniekam ir šādas tiesības:
46.1.pieprasīt šo noteikumu normu skaidrojumu tiešajam vadītājam, DID vadītājam vai pašvaldības IT nodaļas vadītājam;
46.2.pieprasīt tehnisko nodrošinājumu šo noteikumu prasību realizēšanai;
46.3.sniegt priekšlikumus personas datu aizsardzības uzlabošanai;
46.4.pieprasīt konsultācijas un apmācību saistībā ar personas datu apstrādes normatīvo regulējumu un drošību.

47.Darbiniekam ir aizliegts:
47.1.veikt darbības, kas apdraud informācijas resursa vai informācijas sistēmas, kas satur personas datus, drošību;
47.2.bez tiesiska pamata nodot vai izpaust personas datus trešajām personām;
47.3.izmantojot informācijas sistēmu resursus, veikt darbības, kas:
47.3.1.vērstas uz noteikto lietotāja tiesību paplašināšanu;
47.3.2.saistītas ar informācijas resursa drošības sistēmas apiešanu un bojāšanu;
47.3.3.izmantot saņemto informāciju citu datu apstrādes sistēmu izveidei bez saskaņošanas ar DID vadītāju;
48. Darbinieki ir atbildīgi par pašvaldības vai iestādes izdoto rīkojumu, šo noteikumu prasību un citu personas datu apstrādes regulējošo normatīvo aktu prasību neievērošanu, kā par sekām, kas var iestāties personas datu apstrādes pārkāpuma gadījumā.
49.Par šo noteikumu ievērošanu iestādes darbinieki paraksta apliecinājumu.

Direktora p.i. J.Bimbere