



SIGULDAS NOVADA PAŠVALDĪBA

ALLAŽU PAMATSKOLA

Reģ.Nr.4312901109, Skolas iela 5, Allaži, Allažu pagasts, Siguldas novads, LV-2154,
tālr.67970954, 67970949, e-pasts: allazu.pamatskola@sigulda.lv, www.allazupamatskola.lv
AS „SEB banka”, konts Nr.LV15UNLA0027800130404, kods UNLALV2X

IEKŠĒJIE NOTEIKUMI

Siguldas novada Allažu pagastā

19.01.2022.

Nr. 01-4/ 30

Allažu pamatskolas datu aizsardzības noteikumi

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

I. Vispārīgie jautājumi

1. Šie noteikumi nosaka Allažu pamatskolas un tās struktūrvienību (turpmāk - iestāde) personas datu aizsardzības kārtību. Siguldas novada pašvaldībā un tās iestādēs ir kopīgs datu apstrādes pārzinis.
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. Tie ir saistoši visiem darbiniekiem, kas iestādē veic personas datu apstrādi.
3. Personas datu aizsardzības politikā lietotie termini:

3.1. **personas dati** – ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu; identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

3.2. **īpašu kategoriju personas dati (sensitīvie dati)** - dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisku datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju, kā arī dati, kas saistīti ar adoptiju vai aizbildņa iecelšanu;

3.3. **datu subjekts** – fiziska persona, kuru var tieši vai netieši identificēt;

3.4. **trešā persona** – fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.

3.5. **apstrādātājs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā un uzdevumā apstrādā personas datus;

3.6. **personas datu apstrāde** - jebkura ar personas datiem veikta darbības vai darbību kopums, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtīt,

izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

3.7. datu subjekta piekrišana —brīvi, nepārprotami izteikts gribas apliecinājums, ar kuru viņš atļauj apstrādāt personas datus atbilstoši pārziņa sniegtajai informācijai;

3.8. personas datu aizsardzības pārkāpums – ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

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 Siguldas novada pašvaldības personas datu apstrādes darbību reģistrā (turpmāk – Datu apstrādes reģistrā). Personas datu apstrādes darbību reģistru ar rīkojumu apstiprina pašvaldības izpilddirektore.
6. Iestādē tiek apstrādāti tikai tādi personas dati, kas ir atbilstoši Datu apstrādes reģistrā noteiktajiem mērķiem un noteiktajam datu apjomam.
7. Jaunu, Datu apstrādes 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.
9. Iestāde apstrādājot personas datus ievēro šādus principus:
 - 9.1. dati tiek apstrādāti likumīgi un godprātīgi;
 - 9.2. datu apstrāde tiek veikta noteiktiem datu apstrādes nolūkiem un tikai saskaņā ar tiem;
 - 9.3. datu apjoms ir adekvāts un atbilstošs datu apstrādes nolūkam;
 - 9.4. dati ir precīzi un tiek atjaunoti;
 - 9.5. dati netiek glabāti ilgāk nekā nepieciešams;
 - 9.6. dati tiek apstrādāti, ievērojot datu subjekta tiesības;
 - 9.7. dati ir drošībā (nav bez tiesiska pamata pieejami nepilnvarotām trešajām personām);
 - 9.8. dati netiek pārsūtīti ārpus ES/EEZ (Eiropas Savienība / Eiropas ekonomiskā zona) bez adekvātas aizsardzības.
10. Datu apstrāde ir atļauta, ja pastāv kāds no šādiem nosacījumiem:
 - 10.1. datu subjektam tiek nodrošināta pieeja informācijai par nepieciešamo personas datu apstrādi (elektroniski – www.sigulda.lv, sadaļā “Privātuma politika” vai dokumenta formātā iestādē);
 - 10.2. apstrāde ir vajadzīga, lai izpildītu uz iestādi attiecināmu juridisku pienākumu;
 - 10.3. apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;
 - 10.4. datu apstrāde nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;
 - 10.5. datu apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras;
 - 10.6. ir saņemta datu subjekta piekrišana vienam vai vairākiem datu apstrādes nolūkiem;

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

11. 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 personāla vienība ir izveidota.
12. Datortīkla administratori vai iestādes IT speciālists nodrošina:
 - 12.1. loģiskās aizsardzības pasākumus (paroles, antivīrusi, ugunsdrošību, datu kopijas u.c.);
 - 12.2. informācijas resursu darbības atjaunošanu, ja noticis tehnisko resursu bojājums vai arī informācijas resursa darbība ir tikusi traucēta citu iemeslu dēļ.
 13. Par tehniskajiem resursiem (datortehnikas, serveru u.c., uzturēšanu) ir atbildīgi pašvaldības datortīkla administratori vai iestādes IT speciālists.
 14. Datortīkla administratori vai iestādes IT speciālists nodrošina:
 - 14.1. tehnisko resursu darbību;
 - 14.2. tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.
 15. 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.

IV. 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 apgrūtinā 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 īpašu kategoriju personas datiem - personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētiskie 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.

V. 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.

VI. 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 lietošanas noteikumi, kā arī citi iekšējie noteikumi.
26. Darbinieka vispārīgie pienākumi ir:
 - 26.1. veikt datu apstrādi, ja tai ir tiesisks pamats;

26.2. veikt datu apstrādi atbilstoši Datu apstrādes reģistrā noteiktajiem nolūkiem un tam nepieciešamajā apjomā. Datu apstrāde citiem nolūkiem ir pieļaujama tikai normatīvajos aktos noteiktos gadījumos.

26.3. nodrošināt personas datu pareizību un to savlaicīgu atjaunošanu, labošanu un dzēšanu, ja tiek konstatēts, ka 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 un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu.

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 nepieklūst nepilnvarotas trešās personas.

VII. 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 atbilstoši Datu apstrādes reģistrā noteiktajiem nolūkiem un tam nepieciešamajā apjomā. Datu apstrāde citiem nolūkiem ir pieļaujama tikai normatīvajos aktos noteiktos gadījumos.

28.3. nodrošināt personas datu pareizību un to savlaicīgu atjaunošanu, labošanu un dzēšanu, ja tiek konstatēts, ka 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 neklūst 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.

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

29. Iestāde 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 28. punktā minētās personas pieņem lēmumu par tālāko rīcību ar tehniskajiem resursiem un ārkārtas apstākļu novēršanai piemērojamiem pasākumiem.

IX. Personas datu glabāšanas ilgums

32. Personas dati tiek apstrādāti un glabāti līdz noteiktā personas datu apstrādes nolūka sasniegšanai, saskaņā ar iestādes noteikto lietu nomenklatūru, dokumentu un arhīvu pārvaldības un citu normatīvo aktu prasībām.

33. Pēc dokumentu pārvaldības gada noslēguma, atbildīgie darbinieki veic savā darbībā izveidojušos un lietvedībā pabeigtu lietu, kas satur personas datus, analīzi saskaņā ar to glabāšanas termiņiem un sagatavo pastāvīgi glabājamās lietas nodošanai arhīvā arhivēšanai turpmākai glabāšanai.

34. Darbinieks pēc dokumentu pārvaldības gada noslēguma izdzēš no savā pārziņā esošiem datu nesējiem elektroniski saglabātu informāciju, kas satur personas datus, ja tie vairāk nav nepieciešami datu apstrādes mērķa sasniegšanai.

X. Informācijas nesēju glabāšanas un iznīcināšanas kārtība

35. Pirms tehnisko resursu (cietie diski, zibatmiņas, CD utt.) nodošanas utilizēšanai, personas dati no tiem dzēšami un 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.
36. 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 pārlicināties par to ievērošanu.
37. 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.

XI. Datu subjekta tiesību realizācija

38. Datu subjektam ir tiesības:
 - 38.1.iegūt informāciju par tās personas datu apstrādi iestādē.
 - 38.2.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.
 - 38.3.pieprasīt datu labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu.
 - 38.4.tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību.
39. 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, atbildes saskaņošanai.
40. Iestāde 37.punktā minēto iesniegumu izskata un atbildi sniedz viena mēneša laikā.
41. Ja ir objektīvs iemesls (piem., pieprasīto datu apjoms, nepieciešamība pieprasīt papildu informāciju, u.c.), iestāde var nosūtīt datu subjektam starpatbildi un pagarināt iesnieguma izskatīšanas termiņu līdz diviem mēnešiem.
42. Iestāde var atteikties izpildīt datu subjekta informācijas pieprasījumu vai tā izpildes nosacījumus, ja informācijas pieprasījums ir acīmredzami nepamatots vai pārmērīgs, jo īpaši to atkārtotā dēļ.
43. Iestāde var uzaicināt datu subjektu, iestādei 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.

XII. Personas datu apstrādes aizsardzības pārkāpumi

44. Par personas datu aizsardzības pārkāpumu darbiniekiem ir pienākums nekavējoties ziņot DID vadītājam.
45. DID vadītājs izvērtē saņemto informāciju un nepieciešamības gadījumā konsultējoties ar IT vadītāju pieņem lēmumu par turpmāko rīcību.
46. Normatīvajos aktos paredzētos gadījumos DID vadītājs par personas datu aizsardzības pārkāpumu sniedz informāciju Datu valsts inspekcijai.
47. DID vadītājs veic personas datu aizsardzības pārkāpumu uzskaiti, norādot kādas darbības ir veiktas, lai novērstu personas datu aizsardzības pārkāpumu vai mazinātu tā kaitīgās sekas.

XIII. Darbinieku tiesības, pienākumi, ierobežojumi un atbildība

48. Darbiniekiem ir šādi pienākumi:
 - 48.1.pieprasīt piekļuvi informācijas resursiem, kas nepieciešami darba pienākumu pildīšanai;

- 48.2.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;
 - 48.3.veikt visus nepieciešamos aizsardzības pasākumus, lai tam pieejamiem personas datiem bez tiesiska pamata nepieklātu trešās personas;
 - 48.4.pamatot darba devējam nepieciešamību piekļūt vai veikto piekļuvi personas datiem un savas darbības kā informācijas sistēmā tā manuālā apstrādē;
 - 48.5.sadarboties un sniegt informāciju pilnvarotām personām datu aizsardzības pārkāpumu izmeklēšanas gadījumā;
 - 48.6.ievēro konfidencialitāti, bez tiesiska pamata nenodot un neizpaust personas datus trešajām personām, kā darba attiecību laikā, tā arī pēc darba attiecību izbeigšanās;
 - 48.7.citi šajos noteikumos minētie pienākumi.
49. Darbiniekam ir šādas tiesības:
- 49.1.pieprasīt šo noteikumu normu skaidrojumu tiešajam vadītājam, DID vadītājam vai pašvaldības IT nodaļas vadītājam;
 - 49.2.pieprasīt tehnisko nodrošinājumu šo noteikumu prasību realizēšanai;
 - 49.3.sniegt priekšlikumus personas datu aizsardzības uzlabošanai;
 - 49.4.pieprasīt konsultācijas un apmācību saistībā ar personas datu apstrādes normatīvo regulējumu un drošību.
50. 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.izmantojot saņemto informāciju citu datu apstrādes sistēmu izveidei bez saskaņošanas ar DID vadītāju;
51. 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.
52. Par šo noteikumu ievērošanu iestādes darbinieki paraksta apliecinājumu.

XIV. Noslēguma jautājumi

- 53. Iestāde regulāri, bet ne retāk kā 1 (vienu) reizi gadā pārbauda un pārskata šo noteikumu atbilstību iestādes veiktajai datu apstrādei apstrādei un normatīvajiem aktiem, nepieciešamības gadījumā veicot atbilstošus grozījumus.
- 54. Atzīt par spēku zaudējušiem Allažu pamatskolas 2018.gada 15.oktobra iekšējos noteikumus Nr. 30 “Kārtība, kādā tiek ievērota fizisko personu datu aizsardzība izglītības iestādē”.

Allažu pamatskolas direktore

Aina Keplere

2021.gada 19.janvāra

Atbilstoši Allažu pamatskolas iekšējiem noteikumiem Nr.01-4/30

„Allažu pamatskolas datu aizsardzības noteikumi”

APLIECINĀJUMS

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies(usies) ar 2021.gada 19. janvāra Allažu pamatskolas iekšējiem noteikumiem Nr.01-4/ 30 „Allažu pamatskolas datu aizsardzības noteikumi” un izprotu to nosacījumus, kā arī apņemos ievērot tajos ietvertās prasības.

2. Apņemos bez tiesiska pamata neizpaust un neizmantot ierobežotas pieejamības informāciju (t.sk. personas datus), savu vai trešo personu interesēs, kā arī apņemos ievērot Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, Fizisko datu apstrādes likuma un citu normatīvo aktu prasības.

3. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanās.

[illegible]