

IEKŠĒJIE NOTEIKUMI

Rīgā

31.10.2025.

Nr. 1-16/13

Personas datu apstrādes un aizsardzības kārtība

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

I. Vispārīgie noteikumi

1. Personas datu apstrādes un aizsardzības kārtības (turpmāk – Kārtība) mērķis ir nodrošināt SIA “Latvijas Tālmācības un profesionālās tālākizglītības centrs”, vienotais reģistrācijas Nr. 43603054570, tās struktūrvienības Profesionālās tālākizglītības centrs “Latvijas Tālmācības profesionālais centrs”, reģistrēta izglītības iestāžu reģistrā ar Nr. 4461802401 (turpmāk – LTPC) fizisko personu datu apstrādes drošību atbilstoši Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, un ar ko atceļ Direktīvu 95/46 EK un Personas datu apstrādes likuma prasībām (turpmāk – likums) un citiem normatīvajiem aktiem.
2. Definīcijās
 - 1) Kaitnieciska programmatūra – jebkāda programmatūra (piemēram, vīrusi, ļaunprogrammas, spieģļprogrammas, izspiedējprogrammas), kas paredzēta informācijas resursu darbības traucēšanai, datu bojāšanai, iznīcināšanai vai nesankcionētai piekļuvei. Šis termins tiek lietots konsekventi visos LTPC iekšējos normatīvajos aktos.
 - 2) Drošības incidents – jebkāda situācija, kuras rezultātā notikusi nejauša vai nelikumīga personas datu iznīcināšana, zudums, izmaiņas, nesankcionēta piekļuve, izpaušana vai citas darbības, kas apdraud personas datu drošību.
3. Kārtība nosaka, kā LTPC:
 - 3) notiek personas datu apstrāde, aprīte, glabāšana un iznīcināšana;
 - 4) tiek nodrošināti minimālie tehnoloģiskie un organizatoriskie pasākumi personas datu apstrādē;
 - 5) datu subjekts var piekļūt personas datiem kas par to savākti, kādas ir datu subjekta tiesības uz savu personas datu labošanu un “tiesībām tikt aizmirstam”, ja šādu personas datu glabāšana pārkāpj Vispārīgo datu aizsardzības regulu vai Eiropas Savienības, vai dalībvalsts tiesību aktus, kas ir piemērojamas pārzinim;
 - 6) rīkoties gadījumos, kad tiek konstatēts drošības pārkāpums, kas izraisa nejaušu vai nelikumīgu personas datu, kas tiek pārsūtīti, glabāti vai citādi apstrādāti, bojāeju, zudumu, izmaiņas, neatļautu izpaušanu vai piekļuvi tiem;
 - 7) tehniskās un organizatoriskās personas datu aizsardzības prasības papildus nosaka “LTPC IT drošības noteikumi” un “LTPC IT lietošanas noteikumi”. Šī Kārtība lasāma un piemērojama kopā ar minētajiem dokumentiem.
4. Kārtības mērķis ir nodrošināt 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.

5. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam LTPC darbinieku lokam un uz kuriem attiecināms dienesta noslēpuma ievērošanas pienākums. Datu klasifikācija noteikta "Personas datu aizsardzības klasifikatorā" (1.pielikums).
6. Kārtība ir saistoša viesiem LTPC darbiniekiem, kuri apstrādā personas datus.
7. Personas datu apstrāde tiek veikta LTPC telpās un/vai LTPC pārvaldībā esošajās informācijas sistēmās.
8. Kārtība attiecināma uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.
9. Pārzinis var bez brīdinājuma dzēst vai mainīt darbinieka personas datus personas datu apstrādes sistēmas piekļuvei, ja darbinieks pārkāpj Latvijas Republikas normatīvos aktus un/vai saistošos normatīvos aktus, un/vai LTPC iekšējos normatīvos aktus.
10. Pārzinis ir tiesīgs pieprasīt no darbinieka rakstveida apliecinājumu (2.pielikums), par šo noteikumu un konfidencialitātes prasību ievērošanu darbā ar personas datiem un personas datu apstrādes sistēmu, kā arī veikt citas darbības, kuras uzskata par nepieciešamām, lai tiktu ievēroti spēkā esošie Latvijas Republikas normatīvie akti attiecībā uz prasībām par personas datu aizsardzību.
11. Pārziņa pienākums ir rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot darbiniekiem drošu piekļuvi, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.
12. Personas datu apstrāde LTPC notiek, ievērojot šādus pamatprincipus:
 - 8) godprātīga un likumīga datu apstrāde;
 - 9) datu apstrāde tiek veikta atbilstoši paredzētajam mērķim un tikai saskaņā ar to;
 - 10) dati ir adekvāti (ne pārmērīgi);
 - 11) dati ir precīzi;
 - 12) dati netiek glabāti ilgāk kā nepieciešams (datu apstrādes ilgumam ir jābūt saistītam ar noteiktu personas datu apstrādes mērķi);
 - 13) dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;
 - 14) dati ir drošībā;
 - 15) dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas adekvātas aizsardzības.
13. Personas datu apstrādes nolūki:
 - 1) **līguma noslēgšana un izpilde** – lai LTPC varētu noslēgt un izpildīt līgumu, pakalpojuma izpildīšanai, apkopojot un apstrādājot noteiktus personas datus, kas tiek savākti pirms līguma noslēgšanas vai jau noslēgtā līguma laikā;
 - 2) **LTPC leģitīmās intereses** – ievērojot LTPC intereses, kuru pamatā ir kvalitatīva pakalpojuma nodrošināšana. LTPC ir tiesības apstrādāt personas datus tādā apjomā kādā tas ir objektīvi nepieciešams un pietiekams norādīto nolūku īstenošanai;
 - 3) **juridisko pienākumu izpilde** – LTPC ir tiesīga apstrādāt personas datus, lai izpildītu spēkā esošos Latvijas Republikas normatīvos aktus, kā arī sniegtu atbildes uz valsts un pašvaldības likumīgiem pieprasījumiem;
 - 4) **piekrišana** – personas datu subjekta piekrišana personas datu vākšanai un apstrādei noteiktiem mērķiem. Datu subjektam tiesības jebkurā laikā atsaukt savu iepriekš sniegto piekrišanu, izmantojot norādītos saziņas kanālus ar LTPC. Pieteiktās izmaiņas stājas spēkā 3 (trīs) darba dienu laikā pēc šāda paziņojuma saņemšanas. Piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma;
 - 5) **vitālu interešu aizsardzība** – LTPC ir tiesīga apstrādāt personas datus, lai aizsargātu datu subjekta, tā pārstāvju, LTPC darbinieku vai citu fizisku personu vitālās intereses, piemēram, ja apstrāde nepieciešama humanitāros nolūkos, dabas stihiju vai cilvēka izraisītu apdraudējumu (piemēram, epidēmiju un to izplatības uzraudzības), kā arī ārkārtas humanitāro situāciju (piemēram, terora aktu, kibernetizāciju, tehnogēno katastrofu u. c.) gadījumos;
 - 6) **oficiālo pilnvaru izpilde vai LTPC intereses** – LTPC ir tiesīga apstrādāt personas datus, lai izpildītu uzdevumu, ko veic LTPC interesēs vai īstenojot LTPC likumīgi piešķirtās oficiālās pilnvaras. Šādos gadījumos pamats personas datu apstrādei ir iekļauts normatīvajos

aktos. Par personas datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild LTPC valdes loceklis, kurš pats vai ar norīkoto personu starpniecību kontrolē personas datu apstrādes sistēmu drošību.

14. Uzsākot jaunus pamatdarbības virzienus vai jaunus projektus, ir jādefinē paredzamie datu apstrādes mērķi un paredzamais datu apstrādes apjoms, kas nevar būt lielāks par personas datu apstrādes mērķa sasniegšanai nepieciešamo.
15. LTPC izmanto personas datu apstrādē sekojošus personas datu veidus:
 - 1) **identifikācijas un kontaktinformācijas dati:** vārds, uzvārds, personas kods, dzimšanas datums, pases dati, dzimums, adrese, telefona numurs, e-pasta adrese, dzīvesvietas adrese;
 - 2) **pakalpojuma sniegšanas laikā iegūtie dati:** pakalpojuma sniegšanas laikā iegūtie dati, tajā skaitā veselības dati (personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli);
 - 3) **ar pakalpojuma apmaksu saistītie dati:** apmaksas statuss, diagnozes kods, apdrošināšanas polises numurs;
 - 4) **pilnvaroto personu dati:** pilnvarotās personas, kas normatīvajos aktos noteiktajā kārtībā pārstāv datu subjektu.

II. Atbildīgās personas par personas datu apstrādi

16. Par personas datu apstrādi informācijas un tehniskajos resursos, kā arī par personas datu aizsardzību atbildīgās personas LTPC nosaka ar Profesionālās tālākizglītības centra „Latvijas Tālmācības profesionālais centrs” direktora rīkojumu.
17. Atbildīgā persona par informācijas resursiem:
 - 1) nodrošina loģiskās aizsardzības pasākumus;
 - 2) nodrošina informācijas resursu darbības atjaunošanu, ja noticis tehnisko resursu bojājums vai arī informācijas resursu darbība ir tikusi traucēta citu iemeslu dēļ.
18. Atbildīgā persona par tehniskajiem resursiem:
 - 1) nodrošina fiziskās aizsardzības pasākumus;
 - 2) nodrošina tehnisko resursu darbību;
 - 3) nodrošina tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.
19. Atbildīgā par personu datu aizsardzību:
 - 1) organizē un kontrolē personas datu apstrādes atbilstību likuma prasībām;
 - 2) atbild par personāla dokumentācijas un ar to saistīto personas datu apstrādes atbilstību normatīvo aktu prasībām;
 - 3) nodrošina un kontrolē personāla dokumentācijas un tajā iekļauto personas datu apstrādes atbilstību likuma prasībām;
 - 4) nodrošina ar personāla vadību saistīto procesu atbilstību likuma prasībām, tajā skaitā attiecībā uz minētajos procesos veikto personas datu apstrādi.

III. Vispārējā personas datu apstrādes kārtība

20. Pārzinis veic personas datu apstrādi gan manuāli (papīra formā, iekļaujot tos līgumos, vēstulēs, aktos u.c. dokumentos), gan elektroniski, apstrādājot personas datus LTPC grāmatvedības uzskaites programmās.
21. Personas datu vākšanu no datu subjektiem veic LTPC darbinieki, kas strādā ar datu subjektu personas datiem, ievērojot šos Noteikumus, Regulas un citu personas datu apstrādi regulējošo normatīvo aktu prasības.
22. Personas dati no datu subjektiem tiek ievākti datu subjektam uzrādot personas apliecinātos dokumentus, savstarpējās pārrunās, no elektroniskās sarakstes, kā arī aizpildot un iesniedzot attiecīgus dokumentus saskaņā ar spēkā esošajiem Latvijas Republikas normatīvajiem aktiem.
23. Gatavojot līgumu projektus darbiniekiem ir tiesības un pienākums pieprasīt no datu subjekta, lai tiek uzrādīti personu apliecināši dokumenti (pases, personas identifikācijas kartes u.c.) oriģināli. Nav atļauts izgatavot un glabāt minēto dokumentu kopijas.

24. Darbiniekam pirms personas datu saņemšanas ir jāinformē datu subjekts par paredzēto personas **datu apstrādes mērķi** un pamatojums, kā arī jāpārlicinās, ka ir saņemta datu subjekta nepārprotama piekrišana personas datu apstrādei, ja šāda piekrišana nepieciešama.
25. Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu personas datu apdraudējumu.
26. Darbiniekam ir aizliegts glabāt personas datus privātajās ierīcēs (privātos datoros, mobilajos tālruņos, planšetēs) vai privātajos mākoņpakalpojumos (piemēram, Google Drive, Dropbox, iCloud). Personas dati glabājami tikai LTPC pārvaldītajos informācijas resursos.
27. Pārzinis nodrošina tehnisko resursu fizisku aizsardzību pret ārkārtas apstākļiem (ugunsgrēks, plūdi un citi ārkārtas apstākļi). Pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar LTPC ugunsdrošības noteikumiem, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.
28. Lai izvairītos no tehnisko resursu tīšas bojāšanas radītām sekām, Pārzinis rūpējas, lai tehnisko resursu pārvaldība notiktu atbilstoši “LTPC IT drošības noteikumi” (3.pielikums) un “LTPC IT lietošanas noteikumi” (4.pielikums).
29. LTPC personas datu aizsardzības sistēma tiek veidota tā, lai pēc iespējas izvairītos no vienu un to pašu datu apstrādes vairākās struktūrvienībās.
30. Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei tiek iedalīta šādi:
 - 1) konfidenciali dati ir īpašas kategorijas personas dati – šo datu apzīmējums ir K1, kas atbilst augstākajam konfidencialitātes līmenim;
 - 2) iekšējās lietošanas dati ir visi personas lietā iekļautie vai iekļaujamie dati – šo datu apzīmējums ir K2, kas atbilst vidējam konfidencialitātes līmenim;
 - 3) brīvi iekšējās lietošanas dati ir personas vārds, uzvārds, amats, darba vietas e-pasts, darba vietas tālrunis, struktūrvienības nosaukums – šo datu apzīmējums ir K3, kas atbilst zemākajam konfidencialitātes līmenim.
31. Konfidencialie dati tiek apstrādāti tikai, ja to nosaka normatīvie akti un tajos noteiktajā apmērā. Augstākā līmeņa konfidencialie dati (K1) dati tiek marķēti ar apzīmējumu “SENSITĪVS” un tiem tiek piemērots augstākais konfidencialitātes līmenis. Tie tiek izpausti tikai personām, normatīvajos aktos noteikto fiziskās personas tiesību vai pienākumu īstenošanai. Augstākā līmeņa konfidencialie dati (K1) uzglabājami slēgtā telpā vai arī šifrētā veidā, ja tie ir elektroniskā formātā un tiem var piekļūt tikai iepriekš reģistrējoties. Ja konfidencialie dati tiek izmantoti koleģiālo institūciju lēmumu pieņemšanā, publiskojamā lēmuma daļā konfidencialie dati tiek ar fiziskiem un tehnoloģiskiem līdzekļiem slēpti.
32. Iekšējās lietošanas dati un brīvi iekšējās lietošanas dati tiek apstrādāti, ievērojot vispārējos datu apstrādes principus.
33. Pēc datu subjekta pieprasījuma darbiniekam ir pienākums sniegt šādu informāciju:
 - 1) iespējamie personas datu saņēmēji;
 - 2) datu subjekta tiesībām piekļūt saviem personas datiem un izdarīt tajos labojumus.
34. Darbinieks, kas atbild par grāmatvedības vajadzībām ievāko personas datu apstrādāšanu, apstrādā šos personas datus, veicot to reģistrāciju, sakārtošanu, pārveidošanu, nodošanu, kopēšanu un cita veida apstrādi. Pārējiem darbiniekiem piekļuves tiesības noteiktas “Personas datu aizsardzības klasifikatorā” ar tiesībām vai bez tiesībām veikt jebkādas grozījumus vai izmaiņas tajos.
35. Darbinieki ir atbildīgi par personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi, kā arī nodrošina personas datu uzglabāšanu, sniegšanu, izpaušanu un nodošanu saskaņā ar Regulā, citos normatīvajos aktos un šajos noteikumos minētajām prasībām.
36. Darbinieki nododot personas datus, nodrošina informācijas saglabāšanu par:
 - 1) personas datu nodošanas laiku;
 - 2) personu, kas nodevusi personas datus;
 - 3) personu, kas saņēmusi personas datus;
 - 4) personas datiem, kas tikuši nodoti.
37. Informācija tiek saglabāta rakstveidā, saskaņā ar LTPC dokumentu klasifikācijas shēmu.

38. Darbiniekiem ir pienākums nekavējoties ziņot LTPC valdei un tehnisko resursu turētājam par izmantojamās datu apstrādes sistēmas nepilnībām, drošības incidentiem, iespējamiem darbības traucējumiem, kā arī ziņot par iespējamo pārkāpumu personas datu apstrādē.
39. Darbiniekiem nav atļauts bez saskaņojuma ar LTPC valdi veikt personas datu iznīcināšanu.
40. Faksu, skeneru un distances saziņas līdzekļu, kurus izmantojot iespējams individuāls kontakts ar datu subjektu, ir atļauts izmantot saziņai ar datu subjektu tikai tādos nolūkos, kas noteikti šajā Kārtībā vai ja šādas tiesības noteiktas līgumā un/vai likumā. Izmantojot tālruni, atbildīgā darbinieka (pilnvarotās personas) pienākums ir sarunas sākumā informēt datu subjektu par savu identitāti un zvana mērķi. LTPC aizliegta šādu sarunu ierakstīšana, šādu ierakstu glabāšana un izmantošana.
41. Personas datus saturošie dokumenti jāglabā slēdzamā skapī (vēlams metāla). Atslēga tiek glabāta pie atbildīgā darbinieka.
42. Ne retāk kā reizi gadā ir jāveic personas datu apstrādes mērķa un ar to saistīto datu apjoma izvērtējums, ko veic LTPC valde vai pilnvarotā persona.
43. Ja tiek saņemts pieprasījums no datu subjekta par informācijas iegūšanu par personu datu apstrādi, kas saistīta ar viņu, tad pēc LTPC valdes locekļa pieprasījuma, atbildīgais darbinieks apkopo visu informāciju, kas saistīta ar datu subjekta personu datu apstrādi un nodod to LTPC valdes loceklim, kas saņemto informāciju apkopo izziņas veidā un izsniedz datu subjektam.
44. Par personas datu apstrādes aizsardzības uzraudzību un nodrošināšanu atbilstoši šai Kārtībai ir atbildīgs LTPC valdes loceklis, kura pārziņā tiek organizēta datu apstrāde, un par attiecīgo datu apstrādi – pilnvarotais darbinieks jeb pakalpojuma sniedzējs.
45. Darbiniekam ir aizliegts nodot vai ļaut piekļūt personas datiem personām, kurām šāda piekļuve nav nepieciešama tiešo darba pienākumu izpildei.
46. Darbiniekam pienākums bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību izbeigšanas.
47. Darbiniekam pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to pretlikumīgu apstrādi.
48. Kārtībā noteikto datu apstrādes pamatprincipu pārkāpšana, tai skaitā, jebkādā veidā iegūto personas datu neatļauta izpaušana, ir uzskatāma par LTPC iekšējās kārtības noteikumu pārkāpumu.

IV. Personas datu apstrāde informācijas resursos

49. Informācijas sistēmās personas datu apstrādes loģisko drošību nodrošina LTPC valdes loceklis, organizējot drošības iestatījumus tā, lai iespējamie riski tiktu novērsti pirms to iestāšanās.
50. Personas datu aizsardzību informācijas nesējos īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu personas datu apdraudējumu.
51. Personas datu apstrādes sistēmas datortehnikas un programmatūras tehniskā uzstādīšana un tās administrēšana tiek nodrošināta atbilstoši LTPC IT drošības noteikumiem un LTPC IT lietošanas noteikumiem.
52. Piekļuve informācijas resursiem tiek ierobežota ar paroli:
 - 1) parole veidojama no vismaz astoņiem simboliem, starp kuriem ir vismaz viens latīņu alfabēta mazais burts, vismaz viens latīņu alfabēta lielais burts un vismaz viens cipars;
 - 2) paroli aizliegts veidot, izmantojot ar sistēmas lietotāju saistītu informāciju (piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, mājdzīvnieku un tuvinieku vārdus u. tml.);
 - 3) paroli ieteicams mainīt ne retāk kā reizi trijos mēnešos;
 - 4) parole nedrīkst būt pieejama trešajām personām. Paroli nedrīkst uzglabāt pierakstītu uz papīra vai arī elektroniskā formā, ja tas rada apdraudējumu parolei nokļūt trešās personas rokās;
 - 5) attālināta piekļuve informācijas resursiem caur internetu tiek aizsargāta ar lokālā tīkla maršrutētāju, kam ir ugunsbūvē funkcija.
53. Datorizētās informācijas sistēmām tiek nodrošināta autentifikācija atbilstoši LTPC IT drošības noteikumiem.

54. Apstrādājot personas datus informācijas sistēmā, tiek nodrošināta tikai atbilstošo darbinieku piekļūšana pie tehniskajiem līdzekļiem un informācijas.
55. Pārzinis personas datu saturošas programmatūras apstrādei lieto šādas ierīces:
 - 1) darbstacijas un portatīvās iekārtas ar operētājsistēmu;
 - 2) citas licencētas iekārtas un programmatūru pēc vajadzības.
56. Darbinieks ir atbildīgs par datortehniku, kas nodota tā rīcībā, kā arī par dokumentiem, kas nepieciešami personas darba pienākumu pildīšanai.
57. Personas datu apstrādāto informācijas resursu uzglabāšana notiek atbilstoši LTPC lietu nomenklatūrai par kuras aktualitāti atbild LTPC valdes loceklis.
58. Darbiniekam ir tiesības izmantot lietošanā nodotos datorus un to programmatūru tikai darba vajadzībām.
59. Darbinieks nedrīkst izpaust ziņas par LTPC datoru tīklu uzbūvi un konfigurāciju, kā arī atklāt ierobežotas pieejamības informāciju nepilnvarotām personām. Personas datus var izpaust, pamatojoties uz rakstveida iesniegumu, norādot datu izmantošanas mērķi, ja normatīvajos aktos nav noteikts citādi. Personas datu pieprasījumā norādāma informācija, kas ļauj identificēt datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjomu. Jebkura informācijas sniegšana iepriekš saskaņojama ar LTPC valdes locekli.
60. Darbiniekam ir aizliegts izmantot nelicencētu programmatūru.
61. Darbinieks nedrīkst izdarīt darbības, kas būtu vērstas pret informācijas sistēmas drošību, izmantojot neparedzētas pieslēgšanās iespējas.
62. Beidzot (pārtraucot) darbu ar informācijas sistēmu, darbinieks aizver pārlūkprogrammu.
63. Darbinieks 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.
64. Ja ir aizdomas par tīšiem bojājumiem, kas ir radušies informācijas sistēmai paroles publiskošanas rezultātā vai citu iemeslu dēļ, pilnvarotā persona par to nekavējoties ziņo LTPC valdes loceklim.
65. Par jebkuru personas datu apstrādes incidentu darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo informācijas resursu un tehnisko resursu turētājam:
 - 1) ja konstatēts jebkāda veida apdraudējums tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);
 - 2) ja konstatēts jebkāda veida apdraudējums informācijas resursiem (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi u.c.).
66. Incidentu gadījumā darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.

V. Datu subjekta tiesības

67. Datu subjektam ir tiesības iegūt visu informāciju, kas par viņu savākta LTPC personu datu apstrādes sistēmā, iesniedzot iesniegumu LTPC valdes loceklim, ja vien šo informāciju izpaust nav aizliegts ar likumu.
68. Datu subjektam ir tiesības iegūt informāciju par tām fiziskām un juridiskām personām, kuras ir saņēmušas informāciju par šo datu subjektu, iesniedzot iesniegumu LTPC valdes loceklim.
69. Datu subjektam ir tiesības pieprasīt arī šādu informāciju:
 - 1) pārziņa nosaukums, adrese;
 - 2) personas datu apstrādes mērķis, apjoms, veids;
 - 3) datums, kad klienta personas datus pēdējo reizi ir izdarīti labojumi, dati dzēsti vai bloķēti;
 - 4) personas datu ieguves avots;
 - 5) automatizētajā apstrādes sistēmā izmantotās apstrādes metodes, par kuru piemērošanu tiek pieņemti individuāli automatizēti lēmumi.
70. Datu subjektam ir tiesības pieprasīt, lai viņa personas datus papildina vai izlabo, kā arī pārtrauc to apstrādi vai iznīcina tos, ja personas dati ir nepilnīgi, novecojoši, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami vākšanas mērķim. Datu subjektam minētā prasība ir jāpamato. Ja šāda

prasība izrādās pamatota, tad LTPC ir pienākums nekavējoties novērst šo nepilnību vai pārkāpumu un par to paziņot trešajām personām, kas iepriekš ir saņēmušas apstrādātos datus.

71. Datu subjekta pieprasījums ir jāizskata un ir jāizsniedz rakstveida pamatota atbilde viena mēneša laikā no attiecīgā pieprasījuma iesniegšanas dienas.
72. Datu subjektam ir tiesības iepriekš norādīto informāciju bez maksas saņemt divas reizes gadā, iesniedzot iesniegumu.

VI. Personas datu apstrādes aizsardzības pārkāpumi

73. “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.
74. Paziņojumā jānorāda personas datu aizsardzības pārkāpuma raksturs, tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuvenais skaits, personas datu ierakstu kategorijas un aptuvenais skaits, datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija vai cits kontaktpunkts papildu informācijas iegūšanai, iespējamās pārkāpuma sekas, kā arī pārziņa veiktie vai plānotie pasākumi pārkāpuma novēršanai un, ja nepieciešams, tā seku mazināšanai.
75. Personas datu apstrādes aizsardzības pārkāpuma paziņojumu Datu valsts inspekcijai iesniedz Pārzinis.
76. Personas datu aizsardzības pārkāpuma gadījumā datu pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms iesniedz Personas datu apstrādes aizsardzības pārkāpuma paziņojumu.
77. Datu pārzinis var neiesniegt Paziņojumu gadījumos, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.
78. Ja un ciktāl informāciju nav iespējams sniegt vienlaikus, informāciju var sniegt pa posmiem bez turpmākas nepamatotas kavēšanās. Ja paziņošana Datu valsts inspekcijai nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.
79. Aizpildītu Paziņojuma formu var iesniegt elektroniski parakstītu nosūtot uz Datu valsts inspekcijas oficiālo e-pasta adresi info@dvi.gov.lv ar norādi “Paziņojums par personas datu aizsardzības pārkāpumu”, ierakstītā sūtījumā vai personīgi Datu valsts inspekcijā, kā arī veicot autorizāciju valsts pārvaldes pakalpojumu portālā www.latvija.lv.
80. LTPC kontaktinformācija ar personas datu apstrādi saistītajos jautājumos, kā arī datu subjektu pieprasījumu iesniegšanai un informēšanai par iespējamiem datu aizsardzības pārkāpumiem ir: datu.aizsardziba@ltpc.lv.

VII. Noslēguma jautājumi

81. Ar šo noteikumu spēkā stāšanos zaudē spēku 2018.gada 20.decembra Iekšējie noteikumi Nr. 1-18/1 “Personas datu apstrādes aizsardzības noteikumi”.

Direktore

Iveta Skrastiņa

SASKAŅOTS

SIA „Latvijas Tālmācības un profesionālās tālākizglītības centrs”,
struktūrvienības Profesionālās tālākizglītības centrs

“Latvijas Tālmācības profesionālais centrs”

dibinātāja _____ Ilze Kalniņa

Blomē, 31.10.2025.

Skrastiņa
26694694

PERSONAS DATU AIZSARDZĪBAS KLASIFIKATORS

Nr.p.k.	Dokumenta nosaukums	Konfidencialitātes kategorija	Piekļuves tiesības	Glabāšanas termiņš
1.	Direktora rīkojumi organizatoriskos jautājumos un reģistrs	K3	Izglītības iestādes administrācija, biroja darbinieki	10 gadi EK
2.	Juridisko un fizisko personu iesniegumi, sūdzības un priekšlikumi un reģistrs	K3	Izglītības iestādes administrācija, biroja darbinieki	2 gadi EK
3.	Darbiniekiem un izglītojamiem izsniegtās izziņas un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
4.	Sadarbības līgumi ar organizācijām un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	10 gadi
5.	Dalībnieka lēmumi un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	Pastāvīgi
6.	Direktora rīkojumi personāla jautājumos un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
7.	Rīkojumi par komandējumiem un atvaļinājumiem un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
8.	Darba līgumi (amata apraksti pielikumā), vienošanās par izmaiņām un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
9.	Darbinieku personas lietas (darbinieka anketa, iesniegums par pieņemšanu darbā, obligātās veselības pārbaudes veidlapa, ģimenes ārsta atzinums u.c.)	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
10.	Darbinieku atvaļinājumu grafiks	K3	Izglītības iestādes administrācija, biroja darbinieki	2 gadi
11.	Izsniegtās pilnvaras un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
12.	Uzņēmuma līgumi ar fiziskām personām un reģistrs un darba pieņemšanas - nodošanas akti	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
13.	Autoru līgumi un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
14.	Darbinieku darba aizsardzības instruktāžas žurnāli	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi

15.	Akti vai atzinumi par notikušajiem nelaimes gadījumiem un uzskaites žurnāls	K2	Izglītības iestādes administrācija, biroja darbinieki	45 gadi
16.	Pedagogu tālākizglītības plāns	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
17.	Ētikas komisijas slēdzieni un izskstīto lietu materiāli	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
18.	Rīkojumi par izglītojamiem un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
19.	Izglītojamo reģistrācijas un uzskaites grāmata	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
20.	Izglītojamo personas lietas	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi pēc iestādes beigšanas
21.	Grupu sekmju izraksti (kursu beidzot)	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
22.	Līgumi ar izglītojamajiem par mācībām LTPC un reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	5 gadi pēc LTPC beigšanas
23.	Elektroniskā datu bāze par izglītojamajiem VIIS	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
24.	Grupu mācību priekšmetu ieskaīšu, nodarbību un vebināru grafiki	K3	Izglītības iestādes administrācija, biroja darbinieki	2 gadi
25.	Izglītojamo saraksti pa grupām	K2	Izglītības iestādes administrācija, biroja darbinieki	2 gadi
26.	Drošības instrukcijas izglītojamajiem, pedagogiem	K3	Izglītības iestādes administrācija, biroja darbinieki, klašu audzinātāji	Līdz nomaīnai
27.	Izsniegto profesionālās kvalifikācijas un profesionālās pilnveides izglītības apliecību reģistrs	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
28.	Profesionālās kvalifikācijas eksāmenu protokoli	K2	Izglītības iestādes administrācija, biroja darbinieki	75 gadi
29.	Izglītojamo pilnveides izsniegto kursu/ meistarklašu apliecību reģistrs	K3	Izglītības iestādes administrācija, biroja darbinieki	5 gadi
30.	Ziņojumi par valsts sociālās apdrošināšanas obligātajām iemaksām un iedzīvotāju ienākuma nodokli pārskata mēnesī	K2	Grāmatvedība	5 gadi
31.	Attaisnojošie dokumenti (memoriālie orderi, banku, norēķinu centru izraksti,	K2	Grāmatvedība	5 gadi

	kases attaisnojošie dokumenti, darba algas saraksti u.c.), kuri kalpojuši par pamatojumu grāmatvedības ierakstiem			
32.	Darbinieku personas rēķinu (kontu) kartītes	K2	Grāmatvedība	10 gadi
33.	Algu aprēķinu saraksti	K2	Grāmatvedība	5 gadi
34.	No arhīva izsniegto lietu uzskaites žurnāls	K2	Izglītības iestādes administrācija, atbildīgais par arhīvu	5 gadi
35.	Akti par dokumentu atlasī iznīcināšanai	K2	Izglītības iestādes administrācija, atbildīgais par arhīvu	Pastāvīgi
36.	Akti par lietu pieņemšanu-nodošanu mainoties atbildīgajam par arhīvu	K2	Izglītības iestādes administrācija, atbildīgais par arhīvu	Pastāvīgi

Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei tiek iedalīta šādi:

- 1) konfidenciāli dati ir īpašas kategorijas personas dati – šo datu apzīmējums LTPC risku klasifikatorā ir K1, kas atbilst augstākajam konfidencialitātes līmenim;
- 2) iekšējās lietošanas dati ir visi personas lietā iekļautie vai iekļaujamie dati – šo datu apzīmējums LTPC risku klasifikatorā ir K2, kas atbilst vidējam konfidencialitātes līmenim;
- 3) brīvi iekšējās lietošanas dati ir personas vārds, uzvārds, amats, darba vietas e-pasts, darba vietas tālrunis, struktūrvienības nosaukums – šo datu apzīmējums LTPC risku klasifikatorā ir K3, kas atbilst zemākajam konfidencialitātes līmenim.

[illegible]

LTPC IT DROŠĪBAS NOTEIKUMI

1. VISPĀRĪGIE JAUTĀJUMI

- 1.1. Šie noteikumi nosaka kārtību, kādā LTPC nodrošina informācijas sistēmu, datu un tehnisko resursu drošību, ievērojot GDPR (latviski –Vispārīgā datu aizsardzības regula), Informācijas tehnoloģiju drošības likumu un MK 442.
- 1.2. Noteikumi attiecas uz visiem darbiniekiem, prakses studentiem un sadarbības partneriem, kas izmanto LTPC informācijas resursus.
- 1.3. Noteikumu mērķis – nodrošināt konfidencialitāti, pieejamību un integritāti.

2. TERMINI

- 2.1. Informācijas resursi – dati, datubāzes, serveri, programmatūra, tīkli u.c.
- 2.2. Drošības incidents – jebkāda nesankcionēta piekļuve, datu zudums, kaitnieciska programmatūra u.tml.

3. ORGANIZATORISKIE PASĀKUMI

- 3.1. IT drošību uzrauga IT drošības atbildīgā persona.
- 3.2. Katram darbiniekam tiek piešķirts unikāls lietotājvārds un parole.
- 3.3. Piekļuves tiesības tiek regulāri pārskatītas vismaz reizi gadā.
- 3.4. Darbinieki regulāri apgūst datu aizsardzības un IT drošības apmācības.

4. FIZISKĀ DROŠĪBA

- 4.1. Telpām, kur atrodas datortehnika, jābūt slēdzamām.
- 4.2. Rezerves kopijas glabājamās atsevišķi un aizsargātas pret bojājumiem.

5. LOĢISKĀ DROŠĪBA

- 5.1. Parolēm jābūt vismaz 6 rakstzīmēm, ar lielajiem, mazajiem burtiem un cipariem.
- 5.2. Paroles jāmaina ne retāk kā reizi 90 dienās.
- 5.3. Aizliegts glabāt paroli pierakstītu pie datora vai publiski pieejamu.

6. PROGRAMMATŪRAS DROŠĪBA

- 6.1. LTPC izmanto tikai licencētu programmatūru.
- 6.2. Programmas drīkst instalēt tikai IT atbildīgā persona.

7. E-PASTA UN INTERNETA DROŠĪBA

- 7.1. Darba e-pasts izmantojams tikai darba vajadzībām.
- 7.2. Aizliegts atvērt aizdomīgus pielikumus un izmantot neatļautus mākoņpakalpojumus.

8. REZERVES KOPIJAS

- 8.1. IT atbildīgais nodrošina regulāru datu rezerves kopēšanu.
- 8.2. Rezerves kopijas glabājas atbilstoši datu glabāšanas prasībām.

9. INCIDENTU APSTRĀDE

- 9.1. Par drošības incidentu darbiniekiem nekavējoties jāziņo IT atbildīgajam un vadībai.
- 9.2. Incidents tiek dokumentēts un analizēts.

10. NOSLĒGUMA JAUTĀJUMI

- 10.1. Noteikumi stājas spēkā ar direktora rīkojumu.
- 10.2. Visi darbinieki paraksta apliecinājumu par noteikumu ievērošanu.

LTPC IT LIETOŠANAS NOTEIKUMI

1. VISPĀRĪGIE NOTEIKUMI

1.1. Noteikumi nosaka LTPC datoru, tīkla, e-pasta, interneta un tehnisko līdzekļu lietošanas kārtību.

1.2. Noteikumi saistoši visiem LTPC darbiniekiem un līgumdarbiniekiem.

2. DARBA TEHNIKAS LIETOŠANA

2.1. Datori izmantojami tikai darba vajadzībām.

2.2. Aizliegts instalēt programmas bez atļaujas.

2.3. Darbiniekam jāargā dators no bojājumiem un nesankcionētas piekļuves.

3. E-PASTS

3.1. Darba e-pasts izmantojams profesionālai saziņai.

3.2. Aizliegts nosūtīt personas datus bez droša pamata.

3.3. Aizliegts glabāt sensitīvos datus e-pastā ilgāk, nekā nepieciešams.

4. INTERNETS

4.1. Internets izmantojams darba vajadzībām.

4.2. Aizliegts apmeklēt lapas ar augstu drošības risku (pirātiskas, azartspēļu, pieaugušo).

5. MOBILĀS IERĪCES

5.1. Darba telefoni un planšetes lietojamas atbilstoši noteikumiem.

5.2. Aizliegts uzstādīt privātas un nedrošas lietotnes.

6. DATU GLABĀŠANA

6.1. Darba dokumenti glabājami LTPC failu serveros.

6.2. Aizliegts glabāt darba datus privātajos datoros, telefonos vai mākoņos.

7. DATU NODOŠANA

7.1. Datus drīkst nodot tikai saskaņā ar tiesisku pamatu.

7.2. Aizliegts izmantot privātos e-pastus darba dokumentiem.

8. INCIDENTU ZIŅOŠANA

8.1. Nekavējoties jāziņo par drošības riskiem, ierīču zudumu vai aizdomīgām aktivitātēm.

9. DARBA ATTIECĪBU PĀRTRAUKŠANA

9.1. Pārtraucot darba attiecības, jānodod visa tehnika un piekļuves tiek atslēgtas.

10. ATBILDĪBA

10.1. Pārkāpumi tiek uzskatīti par disciplīnas pārkāpumiem un var radīt materiālu atbildību.