LATVIJAS REPUBLIKAS
IZGLĪTĪBAS UN ZINĀTNES MINISTRIJA
RĒZEKNES TEHNIKUMS

Izglītības iestādes reģistrācijas Nr. 3134003053
Varoņu iela 11a, Rēzekne, LV 4604
Tālr. 646 33 664· Fakss 646 32 665 · e – pasts: pasts@rezeknestehnikums.lv

RĒZEKNE

Apstiprināts ar
Rēzeknes tehnikuma direktora
2020. gada 10. janvāra
rīkojumu Nr.1.12/6A

RĒZEKNES TEHNIKUMA DATU APSTRĀDES UN AIZSARDZĪBAS NOTEIKUMI

Izdoti saskaņā ar
Fizisko personu datu apstrādes likumu

I. Vispārīgie jautājumi

1. Rēzeknes Tehnikuma (turpmāk tekstā- **RT**) datu apstrādes aizsardzības iekšējie noteikumi nosaka datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot RT datu apstrādes drošību atbilstoši Vispārīgās datu aizsardzības regulas un Fizisko personu datu apstrādes likuma prasībām.
2. Noteikumu mērķis ir noteikt RT organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu 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 apstrādes likumu un Informācijas tehnoloģiju drošības likumu uz fizisko personas 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*** — RT, 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), RT vai personas, kuras tieši pilnvarojusi RT;

3.11. ***drošības incidents*** – ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas resursu integritāte, pieejamība vai konfidencialitāte.

4. Datu apstrāde tiek veikta RT telpās un/vai RT pārvaldībā esošajās informācijas sistēmās.
5. Noteikumi saistoši visiem RT darbiniekiem.
6. Noteikumi attiecināmi uz visiem datiem, tai skaitā uz identificētu vai identificējamu fizisko personu.
7. Datu apstrāde RT notiek, ievērojot šādus pamatprincipus:
   7.1. godprātīga un likumīga datu apstrāde;
   7.2. datu apstrāde tiek veikta atbilstoši paredzētajam mērķim un tikai saskaņā ar to;
   7.3. dati ir adekvāti (ne pārmērīgi);
   7.4. dati ir precīzi;
   7.5. dati netiek glabāti ilgāk, nekā nepieciešams (datu apstrādes ilgumam ir jābūt saistītam ar noteiktu personas datu apstrādes mērķi);
   7.6. dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;
   7.7. dati ir drošībā;
   7.8. dati netiek pārsūtīti uz citām organizācijām vai uz ārvalstīm bez drošas adekvātas aizsardzības.
8. Par datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild RT direktors, kurš pats vai ar norīkotas personas starpniecību kontrolē datu apstrādes sistēmu drošību.
9. RT var bez brīdinājuma dzēst vai mainīt pilnvarotās personas datus (personas datu operatora) datu apstrādes sistēmas piekļuvei, ja pilnvarotā persona pārkāpj Latvijas Republikas normatīvos aktus un/vai RT iekšējos noteikumus.
10. RT ir tiesīgs pieprasīt no pilnvarotās personas rakstveida apliecinājumu par šo noteikumu un konfidencialitātes prasību ievērošanu darbā ar datiem un datu apstrādes sistēmu, kā arī veikt citas darbības, kuras uzskata par nepieciešamu, lai tiktu ievērotas normatīvo aktu prasības datu aizsardzības jomā.
11. RT pienākums ir rūpēties par datu apstrādes sistēmas darbību, nodrošinot pilnvaroto personu drošu piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.

II. Datu apstrādes sistēmas nodrošinājums

12. Datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu datu apdraudējumu.
13. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam RT darbinieku lokam. Informācijas sistēmas datus drīkst izmantot tikai RT darbinieks, kuram RT ir devis atļauju ar attiecīgiem piekļuves datiem.

14. Datu apstrādes sistēmas datortehnikas un programmatūras tehniskā uzstādīšana un tās administrēšana tiek nodrošināta atbilstoši informācijas sistēmu lietošanas un drošības prasībām.
15. Datorizētās informācijas sistēmām (turpmāk – *IS*) tiek nodrošināta autentifikācija atbilstoši RT informācijas sistēmu lietošanas un drošības prasībām.
16. Apstrādājot datus informācijas sistēmā, tiek nodrošināta tikai pilnvarotu personu piekļūšana pie tehniskajiem līdzekļiem un informācijas.
17. Informācijas sistēmas datu apstrādes loģisko drošību nodrošina RT direktora vietnieks informātikas jautājumos, organizējot drošības iestatījumus tā, lai iespējamie riski tiktu novērsti pirms to iestāšanās.
18. Papīra formātā esošie dati (dokumenti) tiek uzglabāti aizslēdzamās telpās vai skapjos nodrošinot piekļuvi datiem tikai personām, kuram pienākumu ietvaros ir tiesības tiem piekļūt. Nozīmi zaudējušie dokumenti tiek neatgriezeniski sabojāti izmantojot specializētus tehniskās ierīces.

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

19. Personas datu apstrāde RT ir atļauta tikai tad, ja normatīvajos aktos nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
    19.1. saņemta personas datu subjekta piekrišana;
    19.2. datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
    19.3. datu apstrāde nepieciešama Rēzeknes tehnikumam likumā noteikto funkciju veikšanai;
    19.4. datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;
    19.5. datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti Pārzinim vai pārraidīti trešajai personai;
    19.6. datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu Pārziņa vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.
20. RT nodrošina, ka katram datu veidam ir noteikts un skaidrs apstrādes mērķis un ir noteikts, kādos gadījumos dati var tikt nodoti citām personām un iestādēm. RT nodrošina, ka dati ir drošībā un aizsargāti. Elektroniskai personas datu apstrādei var izmantot tikai LR un RT iekšējos normatīvajos aktos noteiktās informācijas sistēmās, kas ir reģistrētas RT IS reģistrā un personas datu apstrādes reģistrā.
21. RT nodrošina tehnisko resursu fizisku aizsardzību pret ārkārtas apstākļiem (ugunsgrēks, plūdi un citi ārkārtas apstākļi). Pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar RT ugunsdrošības noteikumiem, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.
22. Lai izvairītos no tehnisko resursu tīšas bojāšanas radītām sekām, RT rūpējas, lai tehnisko resursu pārvaldība notiktu atbilstoši informācijas sistēmu lietošanas un drošības prasībām.
23. RT datu aizsardzības sistēma tiek veidota tā, lai pēc iespējas izvairītos no vienu un to pašu datu apstrādes vairākās struktūrvienībās un dažādās IS.
24. Datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei tiek iedalīta šādi:
    24.1. **konfidenciāli dati** ir sensitīvi dati – šo datu apzīmējums ir **K1**, kas atbilst augstākajam konfidencialitātes līmenim;

24.2. **ierobežotas pieejamības dati** tiek noteikti RT Darba kārtības noteikumu pielikumā Nr.8 – šo datu apzīmējums ir **K2**, kas atbilst vidējam konfidencialitātes līmenim;

24.3. **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.

25. Konfidenciālie dati tiek apstrādāti tikai, ja to nosaka normatīvie akti un tajos noteiktajā apmērā. Tie tiek izpausti tikai personām, normatīvajos aktos noteikto fiziskās personas tiesību vai pienākumu īstenošanai. Augstākā līmeņa konfidenciālie dati (K1) uzglabājami slēgtā telpā vai arī šifrētā veidā, ja tie ir elektroniskā formātā un tiem var piekļūt tikai iepriekš reģistrējoties. Ja konfidenciālie dati tiek izmantoti koleģiālo institūciju lēmumu pieņemšanā, publiskojamā lēmuma daļā, konfidenciālie dati tiek ar fiziskiem un tehnoloģiskiem līdzekļiem slēpti.
26. Ierobežotas pieejamības dati tiek apstrādāti, ievērojot normatīvajos aktos un rīkojumos noteikto kārtību.
27. Brīvi iekšējās lietošanas dati, ievērojot datu apstrādes principus, ir pieejami ikvienam RT darbiniekam, un ir publicējami RT mājaslapā.
28. RT savas darba organizācijas un darbības nodrošināšanai nosaka datu apstrādes mērķi, kā arī paredzēto datu apstrādes apjomu, kam jābūt atbilstošam datu apstrādes mērķa sasniegšanai.
29. Katram noteiktajam personas datu apstrādes mērķim ir jāidentificē datu subjekts, personas datu apstrādes veids un lietotāji vai trešās personas, kuras veic personas datu apstrādi.
30. Uzsākot jaunus pamatdarbības virzienus vai jaunus projektus, ir jādefinē paredzamie datu apstrādes mērķi un paredzamais datu apstrādes apjoms, kas nevar būt lielāks par datu apstrādes mērķa sasniegšanai nepieciešamo.
31. Ne retāk kā reizi gadā ir jāveic datu apstrādes mērķa un ar to saistīto datu apjoma izvērtējums, ko veic RT darbinieks, kura pienākumos ir organizēt personas datu aizsardzību sadarbībā ar struktūrvienību vadītājiem un projektu vadītājiem (1. pielikums).
32. Apstrādāto datu uzglabāšana notiek atbilstoši RT lietu nomenklatūrai.
33. Ja tiek saņemts pieprasījums no datu subjekta par informācijas iegūšanu par darbinieka personas datu apstrādi, kas saistīta ar viņu, tad pēc direktora pieprasījuma, personāla speciālists apkopo visu informāciju, kas saistīta ar datu subjekta personu datu apstrādi izziņas veidā un izsniedz datu subjektam.
34. Ja tiek saņemts pieprasījums no datu subjekta par informācijas iegūšanu par izglītojamā personas datu apstrādi, kas saistīta ar viņu, tad pēc direktora pieprasījuma atbilstošais speciālists vai struktūrvienība apkopo visu informāciju, kas saistīta ar datu subjekta personu datu apstrādi izziņas veidā un izsniedz datu subjektam.
35. Par personas datu apstrādes aizsardzības uzraudzību un nodrošināšanu atbilstoši šiem noteikumiem ir atbildīgi RT struktūrvienību vadītāji vai atbildīgie speciālisti, kuru pārziņā tiek organizēta datu apstrāde, un par attiecīgo datu apstrādi pilnvarotais darbinieks.
36. Noteikumos noteikto datu apstrādes pamatprincipu pārkāpšana, tai skaitā, jebkādā veidā iegūto personas datu neatļauta izpaušana, ir uzskatāma par RT darba kārtības noteikumu pārkāpumu.

IV. Pilnvarotās personas tiesības, pienākumi un atbildība

37. Pilnvarotā persona (personas datu operators) ir atbildīga par datortehniku, kas nodota personas rīcībā, kā arī par dokumentiem, kas nepieciešami personas darba pienākumu pildīšanai.

38. Pilnvarotajai personai ir tiesības izmantot lietošanā nodotos datorus un to programmatūru tikai darba vajadzībām.
39. Pilnvarotā persona nedrīkst izpaust ziņas par RT 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 RT direktoru.
40. Pilnvarotā persona nedrīkst atļaut piekļūt personas datiem citām personām, ja tas nav nepieciešams RT tiešo darba pienākumu veikšanai.
41. Pilnvarotās personas pienākums ir saglabāt un bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību izbeigšanas.
42. Pilnvarotās personas pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to pretlikumīgu apstrādi.
43. Pilnvarotā persona nedrīkst izdarīt darbības, kas būtu vērstas pret informācijas sistēmas drošību, izmantojot neparedzētas pieslēgšanās iespējas.
44. Par jebkuru personas datu apstrādes incidentu, avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem, citām personām kļuvusi zināma parole utt.), kas ietekmē IS funkcionēšanu, darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo informācijas resursu un tehnisko resursu turētājam (augstākstāvošam vadītājam un RT direktora vietniekam informātikas jautājumos).
45. Incidentu gadījumā pilnvarotai personai savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.
46. Par visiem personas datu apstrādes drošības incidentiem tiek informēts Personu datu drošības pārvaldnieks, tiek veikta dienesta izmeklēšana un sastādīts akts. Nepieciešamības gadījumā izveido atsevišķu izmeklēšanas grupu turpmākai drošības incidentu analīzei un izmeklēšanai. Incidentu izmeklēšanas dokumenti glabājas pie Personu datu drošības pārvaldnieka.

V. Datu subjekta tiesības

47. Datu subjektam ir tiesības iegūt visu informāciju, kas par viņu savākta RT personu datu apstrādes sistēmā, iesniedzot iesniegumu RT direktoram, ja vien šo informāciju izpaust nav aizliegts ar likumu.
48. Datu subjektam ir tiesības iegūt informāciju par tām fiziskām un juridiskām personām, kuras ir saņēmušas informāciju par šo datu subjektu, iesniedzot iesniegumu RT direktoram.
49. Datu subjekts, iesniedzot iesniegumu, ir tiesības saņemt šo noteikumu 33. un 34. punktā minēto informāciju bez maksas.
50. Datu subjektam ir tiesības pieprasīt, lai viņa personas datus papildina vai izlabo.

VI. NOSLĒGUMA JAUTĀJUMI

51. Tehnikuma administrācija pēc savas iniciatīvas, ievērojot valstī pieņemtās izmaiņas normatīvajos dokumentos par datu apstrādi un aizsardzību, var izstrādāt grozījumus, precizējumus šajos noteikumos.
52. Izmaiņas Rēzeknes tehnikuma datu apstrādes un aizsardzības noteikumos stājas spēkā ar direktora rīkojumu.

1. pielikums

Rēzeknes Tehnikuma
personas datu apstrādes aizsardzības noteikumiem

PAR _____

struktūrvienībā

APSTRĀDĀTAJIEM FIZISKĀS PERSONAS DATIEM

Aizpildot tabulu par attiecīgajā struktūrvienībā vai projektā apstrādātajiem fiziskās personas datiem, vēlams norādīt vismaz šādu informāciju (tabula var tikt precizēta gan izdodot rīkojumu par datu apstrādi, gan struktūrvienību vadītājiem aizpildot pārskatu par iepriekšējo gadu):

1.	Personu kategorija (darbinieki, semināru apmeklētāji utt.).	
2.	Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei.	
3.	Personas dati – precīzi jānorāda, tieši kādi (piemēram: vārds, uzvārds, tālrunis, vecums, personas kods utt.).	
4.	Ar datiem veicamās darbības (vākšana, glabāšana, sistematizēšana – elektroniski, papīra formātā, publiskošana u.c.).	
5.	Datu apstrādes pamatojums (likuma pants/ līgumsaistības/ personas piekrišana u.c.).	
6.	Datu apstrādes mērķis.	
7.	Kur un cik ilgi dati tiek glabāti.	
8.	Kādā veidā tiek organizēta personas piekrišanas izteikšana datu apstrādei un glabāšanai (vai piekrišana izteikta rakstveidā).	
9.	Kādā veidā (ar fiziskiem vai programmatūras līdzekļiem) tiek nodrošināta datu aizsardzība.	
10.	Kas šos datus apstrādā (amats).	
11.	Kam ir piekļuve datiem un cik lielā apjomā.	
12.	Kādos gadījumos personas datus izsniedz trešajām personām.	
13.	Kādā veidā notiek personas datu aktualizēšana un cik bieži.	
14.	Kādā veidā dati tiek iznīcināti.	
15.	Personas tiesības piekļūt saviem personas datiem un izdarīt tajos labojumus.	
16.	Cita nozīmīga informācija (ja nepieciešams).	