



ALYTAUS RAJONO SAVIVALDYBĖS KULTŪROS CENTRO DIREKTORIUS

**ĮSAKYMAS
DĖL INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMO BEI
DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TAVRKOS
PATVIRTINIMO**

2018 m. spalio 22 d. Nr. K2- 20A
Alytus

Vadovaudamasis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, įgyvendindamas 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB,

t v i r t i n u informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės Alytaus rajono savivaldybės kultūros centre tvarką (pridedama).

Direktorė



Eglė Sereičikienė

PATVIRTINTA

Alytaus rajono savivaldybės kultūros centro
direktorius 2019 m. spalio 22d.
įsakymu Nr. K2-20A

ALYTAUS RAJONO SAVIVALDYBĖS KULTŪROS CENTRO INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMO BEI DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Alytaus rajono savivaldybės kultūros centras informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka (toliau – Tvarka) nustato Alytaus rajono savivaldybės kultūros centro (toliau – Įstaigos) informacinių ir komunikacinių technologijų naudojimo darbo vietoje darbo metu taisykles, taip pat darbuotojų stebėsenos ir kontrolės darbo vietoje taisykles bei mastą.

II SKYRIUS INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMAS

2. Įstaiga atsižvelgiant į darbovietėje einamas pareigas savo nuožiūra darbuotojams suteikia darbo priemones (kompiuterį, mobilųjį telefoną, prieigą prie interneto, elektroninį paštą, bei kitą informacinių technologijų ir telekomunikacijų įrangą).

3. Suteiktos darbo priemonės priklauso Įstaigai ir yra skirtos darbo funkcijoms vykdyti.

4. Darbuotojams, kurie naudojami Įstaigos suteiktu elektroniniu paštu, interneto prieiga ir kita informacinių technologijų ir telekomunikacijų įranga, griežtai draudžiama:

4.1. skelbti, platinti Įstaigos konfidencialią informaciją (įskaitant, bet neapsiribojant, autorinės teisės objektus, vidinius Įstaigos dokumentus) internete, jei tai nėra susiję su darbinių funkcijų vykdymu;

4.2. naudoti elektroninį paštą ir interneto prieigą asmeniniams, komerciniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai informacijai, kompiuterių virusams, masinei piktybiškai informacijai (*spam*) siųsti ar kitiems tikslams, kurie gali pažeisti Įstaigos ar kitų asmenų teisėtus interesus;

4.3. parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir programinę įrangą, siųsti duomenis, kurie yra užkrėsti virusais, turi įvairius kitus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą;

4.4. savarankiškai keisti, taisyti informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą;

4.5. perduoti Įstaigai priklausančią informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą tretiesiems asmenims, jei toks perdavimas nėra susijęs su darbinių funkcijų vykdymu ar gali bet koku būdu pakenkti Įstaigos interesams;

4.6. diegti, saugoti, naudoti, kopijuoti ar platinti bet kokią neautorizuotą, neteisėtą, autorinės teisės pažeidžiančią ar asmeninę programinę/kompiuterinę įrangą;

4.7. naudoti įrangą neteisėtai prieigai prie duomenų ar sistemų, sistemų saugumo tikrinimui, skenavimui, kompiuterinio tinklo srauto duomenų stebėjimui;

4.8. atlikti kitus su darbo funkcijų vykdymu nesusijusius ar teisės aktams prieštaraujančius veiksmus.

5. Įstaigos darbuotojams naudojant elektroninio pašto ir interneto resursus asmeniniais tikslais, Įstaiga neužtikrina darbuotojų asmeninės informacijos konfidencialumo.

III SKYRIUS

DARBUOTOJŲ STEBĖSENA IR KONTROLĖ DARBO VIETOJE

6. Įstaiga organizuoja darbo vietoje elektroniniu ar kitokiu būdu vykdomo keitimosi profesine ir tam tikrais atvejais asmenine ar kitokia informacija darbe procesų stebėseną. Organizuodama stebėseną Įstaiga visais atvejais laikosi proporcingumo ir kitų šiame skyriuje nurodytų principų ir stebėsenos priemonės taiko tik tais atvejais, kai iškeltų tikslų kitomis, mažiau darbuotojų privatumą ribojančiomis priemonėmis neįmanoma pasiekti.

7. Stebėsenos ir kontrolės darbo vietoje tikslai:

8.1. Apsaugoti konfidencialius Įstaigos duomenis nuo atskleidimo tretiesiems asmenims;

8.2. Apsaugoti Įstaigos paslaugų gavėjų ir darbuotojų asmens duomenis nuo neteisėto perdavimo tretiesiems asmenims;

8.3. Apsaugoti Įstaigos informacines sistemas nuo įsilaužimų ir duomenų vagysčių, virusų, pavojingų interneto puslapių, kenkėjiškų programų;

8.4. Apsaugoti Įstaigos turtą ir užtikrinti asmenų saugumą Įstaigos patalpose ar teritorijoje;

8.5. Apsaugoti Įstaigos turtinius interesus ir užtikrinti darbo pareigų laikymąsi.

8. Įstaigoje, siekiant šios Tvarkos 8 punkte nurodytų tikslų, yra naudojamos specialios programos, kuriomis yra automatinio būdu išsaugoma informacija apie darbuotojų interneto naršymo istoriją, kuri yra saugoma vieną mėnesį. Saugomi duomenys apie darbuotojų naršymo istoriją nėra nuolatos stebimi, jų peržiūrėjimas vykdomas tik tada, kai kyla pagrįstas įtarimas dėl teisės aktų ar darbo pareigų pažeidimo, ir peržiūrima tik su galimu pažeidimu susiję duomenys.

9. Šia Tvarka darbuotojai iš anksto informuojami, kad Įstaiga gali patikrinti jiems priskirtuose kompiuteriuose ir telefonuose įdiegtų komunikacijos programų (pvz. *Skype, Viber, Messenger, Facebook, Instagram ir kt.*) turinį, kitokį elektroninį susirašinėjimą ir interneto naršymo istoriją tiek, kiek tai yra būtina šioje Tvarkoje numatytiems tikslams pasiekti, laikantis Tvarkos 14 punkte nurodytų principų.

10. Įstaiga pasilieka teisę be atskiro darbuotojo įspėjimo riboti prieigą prie atskirų interneto svetainių, komunikacijos programų ar programinės įrangos. Nepakankant minėtų priemonių, Įstaiga gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto resursų naudojimo reikalavimų šioje Tvarkoje nurodytais tikslais, tiriant incidentus, atiduoti darbuotojų naudojamą įrangą tirti tretiesiems asmenims, kurie teisės aktų nustatyta tvarka turi teisę tokius duomenis gauti.

11. Esant poreikiui, iš anksto informavusi darbuotojus, siekdama šios Tvarkos 8.4 ir 8.5 punktuose numatytų tikslų ir laikantis Tvarkos 14 punkte nurodytų principų, Įstaiga gali taikyti ir kitokias darbuotojų stebėsenos ir kontrolės priemones (pvz. garso įrašymo, transporto priemonės vietos nustatymo ir kt.).

12. Siekdama šiame skyriuje nurodytų tikslų, Įstaiga vadovaujasi šiais principais:

12.1. **Būtinumas** – Įstaiga, prieš taikydama šioje Tvarkoje nurodytas darbuotojų kontrolės formas, įsitikina, kad naudojama kontrolės forma yra neišvengiamai būtina nustatytiems tikslams pasiekti.

12.2. **Tikslingumas** – duomenys renkami nustatytam, aiškiam ir konkrečiam tikslui ir nėra toliau tvarkomi būdu, neatitinkančiu šioje Tvarkoje nurodytų tikslų.

12.3. **Skaidrumas** – Įstaigoje neleidžiamas joks paslėptas vaizdo, elektroninio pašto, naudojimosi internetu ar programomis stebėjimas, išskyrus atvejus, kuriems esant toks stebėjimas leidžiamas pagal įstatymus arba kai pagal įstatymus leidžiami tokie Įstaigos veiksmai, siekiant nustatyti pažeidimus darbo vietoje.

12.4. **Proporcingumas** – asmens duomenys, kurie gaunami vykdant šiame skyriuje nurodytą kontrolę, yra susiję ir nepertekliniai lyginant su nustatytu siekiamu tikslu.

12.5. **Tikslumas ir duomenų išsaugojimas** – bet kokie duomenys, susiję su darbuotojo kontrole, yra tikslūs, jei reikia nuolat atnaujinami ir teisėtai saugomi ne ilgiau nei tai būtina.

12.6. **Saugumas** – Įstaigoje yra įdiegtos atitinkamos techninės ir organizacinės priemonės siekiant užtikrinti, kad bet kokie saugomi asmens duomenys būtų saugūs ir apsaugoti nuo išorinio kišimosi.

IV KONFIDENCIALUMAS IR SAUGUMAS

13. Darbuotojai privalo laikytis Taisyklių nuostatų ir prisidėti įgyvendinant įdiegtas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto naikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

14. Darbuotojai turi laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino eidami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas. Konfidencialumui ir asmens duomenų saugumui užtikrinti darbuotojai pasirašo nustatytos formos konfidencialumo pasižadėjimą (Taisyklių 1 priedas).

15. Pareiga saugoti asmens duomenų paslaptį taip pat galioja darbuotoją paskyrus į kitas pareigas bei pasibaigus darbo santykiams.

16. Įstaigoje taikomos asmens duomenų apsaugos organizacinės ir techninės priemonės:

16.1. Prieiga prie duomenų suteikiama tik tam asmeniui, kuriam duomenys yra reikalingi jo funkcijoms vykdyti;

16.2. Su asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti naudotojui yra suteiktos teisės;

16.3. Užtikrintas slaptažodžių konfidencialumas; jie yra unikalūs; sudaryti iš ne mažiau kaip 8 simbolių, nenaudojant asmeninio pobūdžio informacijos; keičiami ne rečiau kaip kartą per 2 mėnesius.

16.4. Užtikrinama asmens duomenų apsauga nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

16.5. Užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas (apribojamas neįgaliotų asmenų patekimas į atitinkamas patalpas ir pan.);

16.6. Užtikrinama kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.);

16.7. Kontroliuojama prieiga prie asmens duomenų tokiomis organizacinėmis ir techninėmis asmens duomenų saugumo priemonėmis, kurios fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas;

16.8. Užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais;

16.9. Užtikrinama, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis, išskyrus būtinus atvejus, kurių metu būtų naudojamos organizacinės ir techninės asmens duomenų saugumo priemonės, užtikrinančios realių asmens duomenų saugumą;

16.10. Užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas;

16.11. Užtikrinama kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (pvz., antivirusinių programų įdiegimas, atnaujinimas);

16.12. Jeigu asmens duomenys gaunami/teikiami išorinėje duomenų laikmenoje, užtikrinama asmens duomenų saugos kontrolė;

16.13. Asmens duomenys po jų panaudojimo ištrinami;

16.14. Jeigu asmens duomenys gaunami/teikiami elektroniniu paštu: užtikrinama asmens duomenų saugos kontrolė, asmens duomenys po jų panaudojimo ištrinami

16.15. Jeigu asmens duomenys gaunami/teikiami išoriniais duomenų perdavimo tinklais, užtikrinamas saugių protokolų (pvz., SSL)/slaptažodžių naudojimas;

16.16. Jei naudojami mobilieji įrenginiai (pvz., nešiojamieji kompiuteriai, planšetės, išmanieji telefonai) ne duomenų valdytojo ir (ar) duomenų tvarkytojo vidiniame tinkle, užtikrinama, kad juose esantys ypatingi asmens duomenys ir prisijungimo prie duomenų valdytojo ir (ar) duomenų tvarkytojo tvarkomų asmens duomenų informacija apsaugoma tokiomis priemonėmis, kurios atitiktų asmens duomenų atskleidimo keliamą riziką.

17. Jeigu darbuotojas abejoja saugumo priemonių patikimumu, jis turi kreiptis į tiesioginį vadovą ir į direktoriaus įsakymu paskirtą asmenį, atsakingą už asmens duomenų apsaugą Administracijoje. Esant pagrindui, pastarasis asmuo inicijuoja papildomų saugumo priemonių organizavimą.

18. Administracijoje darbuotojai turi užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui,

saugodami dokumentus direktoriaus įsakymais nustatyta tvarka, taip pat vengdami nereikalingų kopijų darymo. Į atskiras Administracijos bylas nesegami ir nearchyvuojami dokumentai ir (ar) jų kopijos, kuriuose nurodomi asmens duomenys, turi būti sunaikinami tokiu būdu, kad šių dokumentų nebūtų galima atkurti ir atpažinti jų turinio. Šiam tikslui Komisijos darbuotojai privalo naudotis dokumentų naikintuvais. Kiti dokumentų ir (ar) jų kopijų, kuriuose nurodomi asmens duomenys, naikinimo būdai gali būti pasirenkami tik nesant objektyvių galimybių naudotis Administracijoje esančiais dokumentų naikintuvais.

19. Nereikalingos kompiuterinės laikmenos, kuriose yra asmens duomenų, turi būti ištrinamos arba kitaip sunaikinamos.

20. Dokumentai su asmens duomenimis ir jų išrašai yra segami į bylos medžiagą.

21. Darbuotojai kurių kompiuteriuose saugomi asmens duomenys arba iš kurių kompiuterių galima prieiti prie šaltinių, kuriuose saugomi asmens duomenys, prieigai prie asmens duomenų privalo naudoti slaptažodžius, kurie yra suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą. Slaptažodžiai turi būti unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, nenaudojant asmeninio pobūdžio informacijos, keičiami ne rečiau kaip kartą per 2 mėnesius.

22. Administracijoje esančios elektroninės bylos, kuriose kaupiami asmens duomenys, gali būti prieinamos tik tiems Administracijos darbuotojams, kuriems suteikta prieiga. Administracijos kompiuteriuose yra įdiegiamos antivirusinės programos ir užtikrinamas jų atnaujinimas.

23. Atsarginės duomenų kopijos daromos kartą per parą ir saugomos atsarginiame serveryje, iš kurio avarinio praradimo atveju duomenys gali būti atkuriami

IV SKYRIUS BAIGIAMOSIOS NUOSTATOS

24 Ši Tvarka peržiūrima ir atnaujinama esant poreikiui arba pasikeitus teisės aktams, kurie reglamentuoja šios srities teisinius santykius.

25 Ši Tvarka yra privaloma visiems Įstaigos darbuotojams. Darbuotojai su šia tvarka bei jos pakeitimais yra supažindinami pasirašytinai arba elektroninėmis priemonėmis ir įsipareigoja jos laikytis. Šios Tvarkos pažeidimai gali būti laikomi darbo pareigų pažeidimais, už kuriuos gali būti taikoma atsakomybė, numatyta Lietuvos Respublikos darbo kodekse.

Pasirašę asmenys patvirtina, kad:

1. Susipažino su Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka.

2. Laisva valia sutinka, kad būtų atliekamas vaizdo stebėjimas ir fiksavimas Tvarkoje nustatyta tvarka ir tikslais.

Vardas, pavardė	Data	Parašai
		1. Susipažinimą su Tvarka patvirtinu: _____ Parašas 2. Sutikimą, kad būtų atliekamas mano naudojamų darbo priemonių stebėjimas bei vaizdo stebėjimas ir fiksavimas, patvirtinu: _____ Parašas
		1. Susipažinimą su Tvarka patvirtinu: _____ Parašas 2. Sutikimą, kad būtų atliekamas mano naudojamų darbo priemonių stebėjimas bei vaizdo stebėjimas ir fiksavimas, patvirtinu: _____ Parašas
		1. Susipažinimą su Tvarka patvirtinu: _____ Parašas 2. Sutikimą, kad būtų atliekamas mano naudojamų darbo priemonių stebėjimas bei vaizdo stebėjimas ir fiksavimas, patvirtinu: _____ Parašas
		1. Susipažinimą su Tvarka patvirtinu: _____ Parašas 2. Sutikimą, kad būtų atliekamas mano naudojamų darbo priemonių stebėjimas bei vaizdo stebėjimas ir fiksavimas, patvirtinu: _____ Parašas
		1. Susipažinimą su Tvarka patvirtinu: _____ Parašas 2. Sutikimą, kad būtų atliekamas mano naudojamų darbo priemonių stebėjimas bei vaizdo stebėjimas ir fiksavimas, patvirtinu: _____ Parašas