PATVIRTINTA
Žuvinto biosferos rezervato direktoriaus 2019 m. kovo 22 d. įsakymu Nr. V- 41

ŽUVINTO BIOSFEROS REZERVATO DIREKCIJOS ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I. SKYRIUS
BENDROSIOS NUOSTATOS

1. Žuvinto biosferos rezervato direkcijos(toliau – Direkcija) taisyklės (toliau – Taisyklės) reglamentuoja pagrindinius reikalavimus, kuriais vadovaujantis turi būti tvarkomi fizinių asmenų asmens duomenys (toliau – asmens duomenys) Direkcijoje.

2.Taisyklės parengtos vadovaujantis:

2.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas) nuostatomis;

2.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ);

2.3. Direktyvos 95/46/EB 29 straipsnio darbo grupės 2017 m. balandžio 4 d. nuomone Nr. 17/EN „Poveikio duomenų apsaugai vertinimo ir veiksmų, vertinant, ar tvarkymas „gali kelti didelį pavojų“ reglamento Nr. 2016/679 tikslais, gairės“;

2.4. kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais saugų asmens duomenų valdymą ir jų tvarkymo teisėtumą.

3. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679, ADTAĮ ir kituose teisės aktuose.

II. SKYRIUS
PAGRINDINIAI ASMENS DUOMENŲ TVARKYMO IR APSAUGOS REIKALAVIMAI

4. Šiose Taisyklėse nurodytų asmens duomenų valdytoja yra Direkcija, kuri užtikrina, kad asmens duomenys Direkcijoje būtų tvarkomi laikantis Reglamente ir kituose teisės aktuose nustatytų asmens duomenų tvarkymo reikalavimų.

5. Fizinio asmens duomenų tvarkymas laikomas teisėtu, jeigu jis atitinka Reglamento 5 ir 6 straipsnių reikalavimus, t.y. asmens duomenys yra tvarkomi, esant iš anksto apibrėžtam ir teisėtam tikslui, tik tokios apimties, kokios reikia nustatytam tikslui pasiekti, ir esant bent vienam iš Reglamento 6 straipsnio 1 dalyje nurodytų teisėto asmens duomenų tvarkymo kriterijų (fizinis asmuo davė sutikimą; vykdoma sutartis tarp fizinio asmens ir duomenų valdytojo; įstatymai įpareigoja tvarkyti fizinio asmens duomenis; tvarkyti duomenis būtina, siekiant užtikrinti teisėtus interesus).

6. Direkcija, siekdama užtikrinti Duomenų tvarkymo teisėtumą, tvarko duomenų tvarkymo veiklos, už kurią atsako, įrašus, t.y. pildo Duomenų tvarkymo veiklos įrašų žurnalą, kurio pavyzdinė forma nustatyta šių Taisyklių 2 Priede. Duomenų veiklos įrašų žurnale nurodoma:

6.1. duomenų valdytojo tapatybė;

6.2. duomenų apsaugos pareigūnas ir jo kontaktiniai duomenys;

6.3. asmenų kategorijos;

6.4. duomenų kategorijos pagal kiekvieną asmenų kategoriją;

6.5. duomenų tvarkymo tikslai ir teisinis pagrindas pagal kiekvieną duomenų kategoriją;

6.6. duomenų gavėjų kategorijos kiekvienai asmenų kategorijai pagal duomenų perdavimo tikslus bei teisinį pagrindą;

6.7. duomenų saugojimo terminai.

7. Duomenų tvarkymo veiklos įrašus rengia ir peržiūri Duomenų apsaugos pareigūnas ne rečiau kaip kartą per pusmetį.

8. Direkcijos darbuotojai turi rinkti, naudoti ir saugoti duomenis tokia apimtimi, kuri nurodyta duomenų tvarkymo veiklos įrašuose.

9. Jei darbuotojas siekia rinkti, naudoti ir saugoti asmens duomenis ne pagal duomenų tvarkymo veiklos įrašus ar pastebi, jog duomenų tvarkymo veiklos įrašai neapima tam tikro duomenų rinkimo, naudojimo ir saugojimo ar neatitinka Reglamento, darbuotojas turi apie tai informuoti Duomenų apsaugos pareigūną ir gauti jo konsultaciją.

10. Jeigu Valstybinė duomenų apsaugos inspekcija, vadovaudamasi Reglamento 30 straipsnio 4 dalimi, kreipiasi į Direkciją dėl duomenų tvarkymo veiklos įrašų registro pateikimo, atsakymą Valstybinei duomenų apsaugos inspekcijai rengia ir atsakyme duomenų tvarkymo veiklos įrašų registrą pateikia Duomenų apsaugos pareigūnas.

11. Direkcija, kaip duomenų valdytoja, privalo:

11.1. užtikrinti Reglamente ir kituose asmens duomenų saugą reglamentuojančiose teisės aktuose nustatytų reikalavimų laikymąsi;

11.2. įgyvendinti duomenų subjekto teises, nustatytas Reglamente;

11.3. įgyvendinti tinkamas organizacines ir technines duomenų saugumo priemones;

11.4. organizuoti Direkcijos darbuotojų mokymus duomenų saugos srityje;

11.5. atlikti kitas Reglamente ir kituose teisės aktuose nustatytas funkcijas.

12. Direkcijos darbuotojai privalo, atlikdami savo funkcijas ir tvarkydami asmens duomenis, privalo laikytis pagrindinių asmens duomenų tvarkymo reikalavimų:

12.1. tvarkyti duomenis, vadovaudamiesi Reglamentu ir kitais Lietuvos Respublikos teisės aktais, reglamentuojančiaus saugų asmens duomenų tvarkymą;

12.2. tvarkyti asmens duomenis tik pareigybės aprašyme nurodytoms funkcijoms vykdyti;

12.3. užtikrinti, kad duomenys nebūtų prarasti;

12.4. užtikrinti, kad duomenys nebūtų atskleisti asmenims, neįgaliotiems jais naudotis. Šis įsipareigojimas taikomas ir pasibaigus darbo santykiams;

12.5. apie galimus informacijos saugumo incidentus nedelsiant informuoti Direkcijos Duomenų apsaugos pareigūną.

13. Direkcijoje už duomenų apsaugos organizavimą ir kontrolę atsakingi asmenys, jų vykdomos funkcijos ir atsakomybės:

13.1. Duomenų apsaugos pareigūnas vykdo Direkcijos direktoriaus 2018 m. liepos 27 d. įsakyme Nr. P1-200 „Dėl duomenų apsaugos pareigūno“ nurodytas funkcijas ir yra atsakingas už Reglamento laikymosi kontrolę;

13.2. Saugos įgaliotinis, paskirtas 2019 m. kovo 13 d. Direkcijos direktoriaus įsakymu Nr. V-30 „Dėl Valstybinės saugomų teritorijų Direkcijos prie Aplinkos ministerijos Informacinių sistemų duomenų saugos įgaliotinio paskyrimo“, atlieka atitikties ir rizikos vertinimą, organizuoja vadovybės vertinamąją analizę bei atlieka kitas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir Valstybinės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, nurodytas funkcijas.

III. SKYRIUS
DUOMENŲ APSAUGOS PAREIGŪNAS

14. Direkcija paskiria Duomenų apsaugos pareigūną, kuris padeda prižiūrėti kaip Direkcijoje laikomasi Reglamento ir kitų Lietuvos Respublikos teisės aktų, reglamentuojančių saugų asmens duomenų valdymą ir jų tvarkymą.

15. Duomenų apsaugos pareigūnas turi būti tinkamai ir laiku (kuo anksčiau) įtrauktas į visus klausimus, susijusius su Duomenų apsaugą Direkcijoje.

16. Duomenų apsaugos pareigūno vardas bei pavardė ir kontaktiniai duomenys turi būti nurodyti Duomenų tvarkymo veiklos įrašuose ir Direkcijos interneto svetainėje. Direkcija apie Duomenų apsaugos pareigūno paskyrimą praneša Valstybinei duomenų apsaugos inspekcijai.

17. Direkcija padeda Duomenų apsaugos pareigūnui vykdyti nurodytas užduotis suteikdama būtinus išteklius, taip pat suteikdama galimybę susipažinti su duomenimis, dalyvauti duomenų tvarkymo operacijose.

18. Duomenų apsaugos pareigūnas atlieka šias užduotis:

18.1. informuoja Direkcijos darbuotojus ir vadovybę apie jų prievoles pagal Reglamentą ir kitus Lietuvos Respublikos teisės aktus, reglamentuojančius saugų asmens duomenų valdymą ir tvarkymą;

18.2. stebi kaip Direkcijoje laikomasi Reglamento;

18.3. koordinuoja, atlieka ir (arba) stebi poveikio duomenų apsaugai vertinimus Direkcijoje;

18.4. atlieka kontaktinio asmens funkcijas asmenims, kurie kreipiasi į Direkciją su Duomenų tvarkymu susijusiais klausimais;

18.6. rengia šias Taisykles, duomenų tvarkymo veiklos įrašus, visas kitas su asmens duomenų apsauga susijusias vidaus taisykles, procedūras, šablonus ir kitus dokumentus, prižiūri jų laikymąsi ir jos periodiškai peržiūri;

18.7. praneša apie esamus ar galimus Reglamento pažeidimus, keliančius pavojų Direkcijos veiklai, bei konsultuoja darbuotojus, atsakingus už šiuos pažeidimus;

18.8. praneša Direkcijos vadovybei, kai nesivadovaujama Duomenų apsaugos pareigūno nuomone;

18.9. atlieka Duomenų saugumo pažeidimų valdymą;

18.10. atlieka asmens teisių įgyvendinimo valdymą;

18.11. atlieka kitas užduotis, susijusias su Direkcijos atitiktimi Reglamento reikalavimams.

19. Teisės ir personalo skyriaus vyriausiasis specialistas, kuris Direkcijoje vykdo ir Duomenų apsaugos pareigūno funkcijas, veiksmus susijusius su duomenu apsauga tiesiogiai derina su Direkcijos direktoriumi.

IV. SKYRIUS
POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

20. Direkcijos darbuotojai privalo prieš protingą terminą informuoti Duomenų apsaugos pareigūną, kai Direkcijoje ketinama kurti, diegti ar naudoti tam tikras informacines ir ryšių technologijas ir (ar) kitus metodus, skirtus rinkti, naudoti ar saugoti asmens duomenis.

21. Duomenų apsaugos pareigūnas, gavęs darbuotojo pranešimą, jį išnagrinėjęs ir derindamas su Direkcijos vadovu turi nuspręsti, ar turi būti atliktas poveikio duomenų apsaugai vertinimas dėl konkrečių informacinių ir ryšių technologijų ir (ar) kitų metodų, skirtų tvarkyti duomenis Direkcijoje.

22. Vertinant, ar turi būti atliekamas poveikio asmens duomenų apsaugai vertinimas, turi būti atsižvelgiama į šiuos kriterijus:

22.1. naujos rūšies informacinės technologijos, kurios pirmą kartą diegiamos Direkcijoje;

22.2. asmenų automatinio vertinimo ir profiliavimo įrankiai;

22.3. jautrių duomenų bazės;

22.4. informacinių ir ryšių technologijų tikrinimo priemonės;

22.5. vaizdo stebėjimo priemonės;

22.6. įrankai skirti asmenis sekti internete;

22.7. nacionalinio, regioninio ar tarptautinio pobūdžio duomenų bazės, kuriose saugomi dideli duomenų kiekiai;

22.8. vaikų ar vyresnio amžiaus žmonių duomenų bazės;

22.9. debesų kompiuterijos įrankiai;

22.10. socialinių tinklų įrankai;

22.11. kitos konkrečios informacinės ir ryšių technologijos ir (arba) kiti metodai, skirti Direkcijai rinkti, naudoti ar saugoti duomenis, kurie kelia pavojų asmenims pagal Reglamentą.

23. Duomenų apsaugos pareigūnas, priėmęs sprendimą atlikti poveikio duomenų apsaugai vertinimą, turi:

23.1. nustatyti, kokia papildoma informacija iš darbuotojų ir (arba) paslaugų teikėjų yra reikalinga siekiant atlikti poveikio duomenų apsaugai vertinimą;

23.2. nustatyti, kurie paslaugų teikėjai, informacinių technologijų saugumo konsultantai ir (arba) kiti tretieji asmenys turi dalyvauti poveikio duomenų apsaugai vertinime bei paprašyti šių trečiųjų asmenų įsitraukti į poveikio duomenų apsaugai vertinimo rengimą;

23.3. per protingą terminą nuo visos reikiamos informacijos gavimo atlikti poveikio duomenų apsaugai vertinimą ir parengti raštišką vertinimo ataskaitą dėl kiekvienos konkrečios informacinės ir ryšių technologijos ir (ar) metodo, užpildant poveikio duomenų apsaugai vertinimo formą, o tais atvejais, kai nusprendžiama poveikio duomenų apsaugai vertinimą pavesti atlikti paslaugų teikėjui, užtikrinti, kad šiuos veiksmus atliktų atitinkamas subjektas;

23.4. pateikti per protingą terminą poveikio duomenų apsaugai vertinimo išvadą darbuotojui (-ams), kuris (-ie) kreipėsi į Duomenų apsaugos pareigūną.

23.5. atlikus poveikio asmens duomenų apsaugai vertinimą, Duomenų apsaugos pareigūnas, užpildo poveikio asmens duomenų apsaugai vertinimo ataskaitą, kurio pavyzdinė forma nustatyta šių Taisyklių 3 priede.

23.6. visais atvejais poveikio asmens duomenų apsaugai vertinimo ataskaita tarnybiniu pranešimu yra pateikiama Direkcijos direktoriui.

V. SKYRIUS
IŠANKSTINĖS KONSULTACIJOS SU VALSTYBINE DUOMENŲ APSAUGOS INSPEKCIJA

24. Jeigu atlikus poveikio asmens duomenų apsaugai vertinimą, buvo nustatyta, kad Direkcijos turimomis asmens duomenų apsaugos priemonėmis nėra galimybių sumažinti kylantį pavojų asmens duomenų saugumui iki priimtino lygio (t.y. likutinė rizika yra didelė), Duomenų apsaugos pareigūnas, vadovaudamasis Reglamento 36 straipsnyje nustatyta tvarka, privalo kreiptis į Valstybinę duomenų apsaugos inspekciją išankstinės konsultacijos.

25. Duomenų apsaugos pareigūnas bendradarbiauja su Valstybine duomenų apsaugos inspekcija ir vykdo Inspekcijos paklausimų valdymą vadovaudamasis šiomis Taisyklėmis ir Reglamentu.

26. Direkcijos darbuotojas gavęs Valstybinės duomenų apsaugos Inspekcijos paklausimą, nedelsiant, bet ne vėliau kaip per 1 (vieną) darbo dieną, informuoja Duomenų apsaugos pareigūną apie tokį paklausimą.

27. Duomenų apsaugos pareigūnas, gavęs Valstybinės duomenų apsaugos inspekcijos paklausimą, turi nedelsdamas atlikti pirminę paklausimo analizę:

27.1. peržiūrėti Inspekcijos paklausimą;

27.2. nustatyti atsakymo į Inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su Darbuotojais ir (ar) Paslaugų teikėjais);

27.3. jei reikia, kreiptis į Inspekciją dėl termino pateikti atsakymą pratęsimo;

27.4. nustatyti, ar yra reikalinga papildoma informacija iš darbuotojų ir, jei taip - paprašyti tokią informaciją pateikti;

27.5. nustatyti, ar Paslaugų teikėjai, išoriniai Duomenų apsaugos pareigūnai, informacinių technologijų saugumo konsultantai ir (ar) tretieji asmenys yra susiję su Valstybinės duomenų apsaugos inspekcijos paklausimu ir, jei taip, paprašyti jų pagalbos rengiant atsakymą į Inspekcijos paklausimą;

27.4. surinkęs visą atsakymui į Valstybinės duomenų apsaugos inspekcijos paklausimą reikalingą informaciją, tačiau jokiu būdu ne vėliau kaip per Inspekcijos nustatytą terminą, Duomenų apsaugos pareigūnas parengia ir pateikia Inspekcijai atsakymą į paklausimą.

VI. SKYRIUS
DUOMENŲ SAUGUMO PAŽEIDIMŲ VALDYMAS

28. Duomenų apsaugos pareigūnas atlieka duomenų saugumo pažeidimų valdymą vadovaudamasis Reglamentu ir šiomis Taisyklėmis.

29. Direkcijos darbuotojas, sužinojęs apie asmens duomenų saugumo pažeidimą, nedelsiant (ne vėliau kaip per 12 valandų) turi informuoti savo tiesioginį vadovą ir Direkcijos Duomenų apsaugos pareigūną apie duomenų saugumo pažeidimą.

30. Jei Duomenų apsaugos pareigūnas gauna iš darbuotojo Taisyklių 29 punkte numatytą pranešimą ar pats pastebi duomenų saugumo pažeidimą, Duomenų apsaugos pareigūnas turi nedelsdamas, bet ne vėliau kaip per 12 (dvylika) valandų, atlikti pirminę duomenų saugumo pažeidimo analizę.

31. Duomenų apsaugos pareigūnas nedelsiant turi išnagrinėti pranešime nurodytas aplinkybes ir įvertinti, ar padarytas asmens duomenų saugumo pažeidimas.

32. Jeigu duomenų saugumo pažeidimo valdymui reikalinga papildoma informacija, Duomenų apsaugos pareigūnas turi paprašyti darbuotojų ir (arba) paslaugų teikėjų suteikti reikiamą informaciją ne vėliau kaip per 24 valandas.

33. Duomenų apsaugos pareigūnas turi užbaigti duomenų saugumo pažeidimo valdymą ne vėliau kaip per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą.

34. Jei Duomenų apsaugos pareigūnas nustato, kad asmens duomenų saugumo pažeidimas padarytas:

34.1. privalo nedelsiant pradėti tyrimą.

34.2 imasi priemonių pažeidimui pašalinti ir (arba) neigiamoms pažeidimo pasekmėms sumažinti (pvz. naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis);

34.3. pasitelkia Direkcijos informacinių sistemų darbuotojus, jei asmens duomenų saugumo pažeidimas yra susijęs su elektroninės informacijos saugos ir kibernetinio saugumo incidentu;

34.4. tiesiogiai informuoja Direkcijos vadovybę.

35. Duomenų apsaugos pareigūnas informaciją apie asmens duomenų saugumo pažeidimą įrašo į šių Taisyklių 4 priede nurodytos formos Asmens duomenų saugumo pažeidimų registravimo žurnalą.

36. Tyrimo pabaigoje Duomenų apsaugos pareigūnas surašo Taisyklių 6 priede nurodytos formos Asmens duomenų saugumo pažeidimo ataskaitą ir tyrimo išvadą (Priedas Nr. 7), kurioje pažymima, ar buvo nustatytas asmens duomenų saugumo pažeidimas. Jei asmens duomenų saugumo pažeidimas nebuvo nustatytas, tyrimas nutraukiamas. Jei asmens duomenų saugumo pažeidimas nustatomas, tyrimą atlikęs asmuo privalo papildom įvertinti gautos informacijos pakankamumą, patikimumą ir teisingumą. Be to turi nustatyti asmens duomenų kategorijas, kurios buvo susijusios su pažeidimu, pažeidimo priežastys, pažeidimo pobūdis, tipas (asmens duomenų konfidencialumo, vientisumo ir (arba) prieinamumo pažeidimas) aplinkybės, apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius, asmens duomenų, kurių saugumas pažeistas, kategorijos (asmens tapatybę patvirtinantys asmens duomenys, prisijungimo duomenys ir

(arba) asmens identifikaciniai numeriai ir kt.) ir apimtis, tikėtinos asmens duomenų saugumo pažeidimo pasekmės, pavojus fizinių asmenų teisėms ir laisvėms;

37. Direkcijos duomenų apsaugos pareigūnas turi pranešti Valstybinei duomenų apsaugos inspekcijai, ne vėliau kaip per 72 valandas nuo sužinojimo apie asmens duomenų saugumo pažeidimą (Priedas Nr. 5), nebent asmens duomenų saugumo pažeidimas neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu Valstybinei duomenų apsaugos inspekcijai nepranešama per 72 valandas, pranešime nurodomos vėlavimo priežastys. Pranešimas apie asmens duomenų saugumo pažeidimą pateikiamas Valstybinės duomenų apsaugos inspekcijos nustatyta tvarka.

38. Asmens duomenų saugumo pažeidimų pranešime aprašomas asmens duomenų saugumo pažeidimo pobūdis, duomenų subjektų kategorijos ir apytikslis skaičius, asmens duomenų įrašų kategorijos ir apytikslis skaičius, nurodomas duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), aprašomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės bei priemonės, kurių buvo imtasi arba pasiūlyta imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, taip pat priemonės galimoms neigiamoms jo pasekmėms sumažinti bei kita svarbi su asmens duomenų saugumo pažeidimu susijusi informacija.

39. Kai dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms (gali būti padarytas kūno sužalojimas, turtinė ar neturtinė žala, gali kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas, padaryta didelė ekonominė ar socialinė žala, kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis, gali būti paviešinti specialių kategorijų, pažeidžiamų fizinių asmenų asmens duomenys, duomenų apsaugos pareigūnas užtikrina, kad apie asmens duomenų saugumo pažeidimą nepagrįstai nedelsiant būtų pranešta duomenų subjektui: duomenų subjektui aiškia ir paprasta kalba aprašomas duomenų saugumo pažeidimo pobūdis, nurodomas duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas), aprašomos tikėtinos asmens duomenų saugumo pažeidimo pasekmės ir priemonės, kurių buvo imtasi arba pasiūlyta imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, taip pat priemonės galimoms neigiamoms jo pasekmėms sumažinti bei pagal galimybes atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip sumažinti galimą neigiamą poveikį (pasikeisti prisijungimo slaptažodžius neteisėtos prieigos prie asmens duomenų atveju ir kt.).

40. Apie asmens duomenų saugumo pažeidimą duomenų subjektui pranešti neprivaloma, jei:

40.1. Direkcija įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems asmens duomenų saugumo pažeidimas turėjo poveikio;

40.2. iš karto po asmens duomenų saugumo pažeidimo teismas ėmėsi priemonių, kuriomis užtikrinama, kad nebegalėtų kilti didelis pavojus duomenų subjektų teisėms ir laisvėms;

40.3. tai pareikalautų neproporcingai daug pastangų. Tokiu atveju vietoj to apie asmens duomenų saugumo pažeidimą paskelbiama viešai arba taikoma panaši priemonė, kuria duomenų subjektai būtų informuojami taip pat efektyviai.

41. Duomenų apsaugos pareigūnas informaciją apie asmens duomenų saugumo pažeidimą įrašo į šių Taisyklių 4 priede nurodytos formos Asmens duomenų saugumo pažeidimų registravimo žurnalą.

42. Duomenų apsaugos pareigūnas registruja visus asmens duomenų saugos pažeidimus Asmens duomenų saugumo pažeidimų registracijos žurnale.

43. Asmens duomenų saugos pažeidimų registracijos žurnalas yra tvarkomas elektronine forma.

VII. SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Taisyklės iš esmės peržiūrimos ne rečiau kaip kartą per metus.

45. Darbuotojai, kurie yra įgalioti tvarkyti asmens duomenis pasirašo Pasižadėjimą saugoti duomenų paslaptį (Taisyklių 1 Priedas). Direkcijos darbuotojai privalo laikytis šių Taisyklių, pagrindinių asmens duomenų tvarkymo reikalavimų bei konfidencialumo ir saugumo reikalavimų. Už Taisyklių pažeidimą darbuotojai atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

46. Šios Taisyklės įsigalioja nuo jos patvirtinimo dienos ir taikoma darbuotojams nuo supažindinimo su Taisyklėmis dienos.

47. Direkcijos darbuotojai su Taisyklėmis supažindinami pasirašytinai.

_____