

PATVIRTINTA

Nacionalinio bendrųjų funkcijų centro
direktoriaus 2018-08-30 įsakymu Nr. V- 86
(Nacionalinio bendrųjų funkcijų centro
direktoriaus 2019-10-01 įsakymo
Nr. V-492 redakcija)

NACIONALINIO BENDRŪJŲ FUNKCIJŲ CENTRO ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Nacionalinio bendrųjų funkcijų centro asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) nustato pagrindinius reikalavimus, kuriais vadovaujantis turi būti tvarkomi fizinių asmenų asmens duomenys (toliau – asmens duomenys) Nacionaliniame bendrųjų funkcijų centre (toliau – NBFC).

2. Taisyklės parengtos vadovaujantis:

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

2.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

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 duomenų tvarkymą.

3. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente ir kituose Lietuvos Respublikos teisės aktuose.

4. Duomenų subjektų asmens duomenis tvarko duomenų valdytojas – NBFC, juridinio asmens kodas 304768872, buveinės adresas Geležinio Vilko g. 12, LT-03163 Vilnius.

II SKYRIUS PAGRINDINIAI DUOMENŲ TVARKYMO REIKALAVIMAI IR PRINCIPAI

PIRMASIS SKIRSNIS DUOMENŲ TVARKYMO REIKALAVIMAI, FUNKCIJOS IR ATSAKOMYBĖS

5. 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, kurios 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. NBFC privalo:

- 6.1. užtikrinti, kad būtų laikomasi Reglamente ir kituose asmens duomenų apsaugą reglamentuojančiuose teisės aktuose nustatytų reikalavimų;
- 6.2. įgyvendinti duomenų subjektų teises, nustatytas Reglamente;
- 6.3. įgyvendinti tinkamas organizacines ir technines duomenų saugumo priemones;
- 6.4. organizuoti NBFC darbuotojams duomenų saugos mokymus;
- 6.5. atlikti kitas Reglamente ir kituose teisės aktuose nustatytas funkcijas.
- 7. NBFC darbuotojai privalo:
 - 7.1. tvarkyti asmens duomenis vadovaudamiesi Reglamentu ir kitais Lietuvos Respublikos teisės aktais, reglamentuojančiais saugų asmens duomenų tvarkymą;
 - 7.2. tvarkyti asmens duomenis tik pareigybės aprašyme nurodytoms funkcijoms vykdyti;
 - 7.3. užtikrinti, kad asmens duomenys nebūtų prarasti;
 - 7.4. užtikrinti, kad, neturint įgaliojimų, asmens duomenys nebūtų keičiami, pildomi, naikinami ar kt.;
 - 7.5. užtikrinti, kad, neturint įgaliojimų, asmens duomenys įvairiose laikmenose nebūtų išnešti iš NBFC patalpų;
 - 7.6. užtikrinti, kad asmens duomenys nebūtų atskleisti asmenims, neįgaliotiems jais naudotis. Šis įpareigojimas taikomas ir pasibaigus darbo santykiams;
 - 7.7. apie galimus informacijos saugumo incidentus nedelsdami informuoti NBFC duomenų apsaugos pareigūną.

ANTRASIS SKIRSNIS BENDRIEJI ASMENS DUOMENŲ TVARKYMO PRINCIPAI

- 8. NBFC veikloje tvarkant asmens duomenis taikomi šie principai:
 - 8.1. tikslo apribojimo principas – NBFC darbuotojai turi tvarkyti asmens duomenis tik tam, kad atliktų savo konkrečias ir teisėtas funkcijas, numatytas jų pareigybės aprašyme;
 - 8.2. duomenų kiekio mažinimo principas – NBFC darbuotojai neturi rinkti, naudoti ir saugoti asmens duomenų, kurie nėra reikalingi jų darbo funkcijoms atlikti;
 - 8.3. prieigos prie asmens duomenų ribojimo principas – nė vienam NBFC darbuotojui ir / ar kitiems įgaliotiems subjektams neturi būti suteikta prieiga prie asmens duomenų, išskyrus tuos atvejus, kai šie duomenys yra būtini jų darbo funkcijoms atlikti;
 - 8.4. skaidrumo principas – darbuotojai turi įsitikinti, kad kiekvienas asmuo, su kuriuo jie susiduria pirmą sykį NBFC, turi išsamią informaciją apie tai, kokių būdu ir kokie jo asmens duomenys yra renkami, naudojami ir saugojami NBFC;
 - 8.5. tikslumo principas – NBFC darbuotojai imasi protingų pastangų, padedančių užtikrinti, kad visi NBFC tvarkomi asmens duomenys būtų tikslūs ir prireikus atnaujinami;
 - 8.6. saugojimo trukmės apribojimo principas – NBFC darbuotojai turi užtikrinti, kad bet kurie asmens duomenys būtų saugojami NBFC tik tam tikrą laikotarpį, kiek tai yra reikalinga;
 - 8.7. saugumo užtikrinimo principas – NBFC darbuotojai turi užtikrinti, kad asmens duomenys būtų renkami, naudojami ir saugojami laikantis vidaus procedūrų ir užtikrinant asmens duomenų apsaugą nuo neleistinos prieigos, neteisėto rinkimo, naudojimo ir saugojimo, netyčinio praradimo ir sunaikinimo.

III SKYRIUS ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI IR TIKSLAI

- 9. NBFC tvarko duomenų subjektų asmens duomenis tik teisėtu, skaidriu būdu toliau nurodytais pagrindais:
 - 9.1. Duomenų subjektas davė sutikimą NBFC, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais.

9.2. Asmens duomenys tvarkomi siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba duomenų subjekto prašymu siekiant imtis veiksmų prieš sudarant sutartį.

9.3. Tvarkyti asmens duomenis NBFC įpareigoja atitinkami teisės aktai.

9.4. Asmens duomenys tvarkomi dėl NBFC teisėto intereso (tik jei duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, nėra už jį viršesni).

10. NBFC, kaip duomenų valdytojas, besilaikantis Reglamento 5 straipsnyje nustatytų principų, tvarko duomenų subjektų asmens duomenis šiais tikslais:

10.1. NBFC buvusių ir esamų darbuotojų, dirbančių pagal darbo sutartis, asmens duomenys tvarkomi vidaus administravimo (darbo sutarčių sudarymo ir vykdymo, buhalterinės apskaitos tvarkymo, materialinių ir finansinių išteklių naudojimo, vidinės komunikacijos) tikslais;

10.2. Kandidatų į NBFC darbuotojus, dirbančius pagal darbo sutartis, asmens duomenys tvarkomi vidaus administravimo (personalo valdymo ir dokumentų valdymo) tikslais.

10.3. Studentų, atliekančių ar siekiančių atlikti praktiką NBFC, asmens duomenys tvarkomi vidaus administravimo (personalo valdymo ir dokumentų valdymo) tikslais.

10.4. Asmenų, pateikusių NBFC skundą, prašymą ar pranešimą, asmens duomenys tvarkomi skundų, prašymų ar pranešimų nagrinėjimo tikslu.

10.5. Fizinį asmenų, pateikusių viešojo pirkimo pasiūlymus NBFC organizuojant ir atliekant viešuosius pirkimus, asmens duomenys, taip pat fizinių asmenų asmens duomenys, nurodyti viešojo pirkimo pasiūlymuose, sudarytose su NBFC sutartyse, taip pat pateikti vykdant sudarytas su NBFC sutartis, tvarkomi viešųjų pirkimų organizavimo ir vykdymo, sutarčių vykdymo tikslais.

10.6. Asmenų, apsilankančių NBFC socialinių tinklų paskyrose („Facebook“, „LinkedIn“), asmens duomenys tvarkomi NBFC socialinių tinklų paskyrų administravimo tikslu;

10.7. NBFC darbuotojų, skambinančių dėl konsultacijos suteikimo telefonu +370 527 40 004, pokalbių įrašai tvarkomi vienodos ir kokybiškos NBFC darbuotojų konsultavimo praktikos užtikrinimo tikslu.

10.8. Informacinės sistemos „E. sąskaita“ duomenų bazėje tvarkomų sąskaitų ir paslaugų gavėjų duomenų tvarkymo tikslai – identifikuoti ir autentifikuoti paslaugų gavėjus, elektroniniu būdu tvarkyti informacinės sistemos duomenis, teikti informaciją duomenų gavėjams apie sąskaitas ir jų apmokėjimo būseną.

10.9. NBFC darbuotojų, dirbančių pagal darbo sutartis, vaizdo duomenys tvarkomi NBFC nuosavybės teise ar kitu teisiniu pagrindu valdomo turto ir asmens duomenų apsaugos užtikrinimo tikslais.

11. NBFC, kaip duomenų tvarkytojas, tvarko asmens duomenis viešojo sektoriaus subjektų (duomenų valdytojų) vardu, vadovaudamasis šiais teisės aktais:

11.1. Lietuvos Respublikos Vyriausybės 2018 m. gegužės 23 d. nutarimu Nr. 488 „Dėl centralizuoto viešojo sektoriaus subjektų buhalterinės apskaitos organizavimo tvarkos aprašo patvirtinimo“. Šiuo teisės aktu reglamentuotas asmens duomenų tvarkymas atliekamas centralizuoto viešojo sektoriaus subjektų buhalterinės apskaitos organizavimo tikslu.

11.2. Lietuvos Respublikos Vyriausybės 2018 m. gegužės 30 d. nutarimu Nr. 507 „Dėl personalo administravimo funkcijų centralizuoto atlikimo tvarkos aprašo patvirtinimo“. Šiuo teisės aktu reglamentuotas asmens duomenų tvarkymas atliekamas centralizuoto viešojo sektoriaus personalo administravimo tikslu.

IV SKYRIUS DUOMENŲ APSAUGOS PAREIGŪNAS

12. NBFC paskiria duomenų apsaugos pareigūną, atsakingą už Reglamento ir duomenų apsaugos įstatymų reikalavimų laikymosi priežiūrą NBFC:

12.1. Duomenų apsaugos pareigūnas turi būti tinkamai ir laiku (kuo anksčiau) įtrauktas į visus klausimus, susijusius su duomenų apsauga NBFC veikloje.

12.2. Duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys turi būti nurodyti duomenų tvarkymo veiklos įrašuose ir NBFC interneto svetainėje adresu <http://nbfc.lrv.lt/lt/asmens-duomenu-apsauga>.

12.3. Duomenų apsaugos pareigūnas dalyvauja atitinkamose darbo grupėse, nagrinėjančiose duomenų rinkimo, naudojimo ir saugojimo problemas NBFC.

12.4. NBFC padeda duomenų apsaugos pareigūnui vykdyti nurodytas užduotis, suteikdamas būtinus išteklius, taip pat suteikdamas galimybę susipažinti su duomenimis, dalyvauti duomenų tvarkymo operacijose ir išlaikyti savo ekspertines žinias.

12.5. Duomenų apsaugos pareigūnas tiesiogiai atskaitingas NBFC direktoriui.

12.6. NBFC paskelbia duomenų apsaugos pareigūno kontaktinius duomenis ir praneša apie juos Valstybinei duomenų apsaugos inspekcijai.

13. Bet kuris NBFC darbuotojas turi kreiptis į duomenų apsaugos pareigūną ir gauti jo konsultaciją šiais atvejais:

13.1. kai darbuotojui reikia konsultacijos dėl atitikties Reglamentui ir duomenų apsaugos įstatymuose nustatytiems reikalavimams;

13.2. kai darbuotojas ketina pirmą sykį NBFC kurti, diegti ar naudoti konkrečias informacines ir ryšių technologijas ir (arba) kitus metodus, siekdamas rinkti, naudoti ar saugoti asmens duomenis;

13.3. kai darbuotojas ketina pirmą kartą NBFC pasitelkti tam tikrą paslaugų teikėją, kuris turėtų prieigą prie NBFC asmens duomenų;

13.4. kai darbuotojas ketina pirmą kartą NBFC rinkti, naudoti ir saugoti tam tikras jautrių duomenų kategorijas;

13.5. kai darbuotojas sužino apie bet kokį buvusį, esamą ar galimą Reglamento, duomenų apsaugos įstatymų ir (arba) šių Taisyklių pažeidimą NBFC;

13.6. kai darbuotojas nustato, kad gali būti reikalinga šių Taisyklių, bet kokių kitų su duomenų apsauga susijusių taisyklių, procedūrų, formų ir / ar kitų dokumentų peržiūra, pakeitimai ir (arba) papildymai;

13.7. kai darbuotojas sužino apie bet kuri esamą ir (arba) galimą Valstybinės duomenų apsaugos inspekcijos paklausimą, laišką, prašymą ir (arba) tyrimą;

13.8. kai darbuotojas sužino apie bet kuri esamą ir (arba) galimą duomenų subjekto paklausimą, laišką, prašymą ir (arba) skundą.

14. Duomenų apsaugos pareigūnas atlieka šias užduotis:

14.1. informuoja NBFC darbuotojus ir vadovybę apie jų prievoles pagal Reglamentą ir kitus duomenų apsaugos įstatymus;

14.2. stebi, kaip NBFC laikomasi Reglamento ir duomenų apsaugos įstatymų;

14.3. rūpinasi asmens duomenų rinkimo, naudojimo ir saugojimo veikloje dalyvaujančių darbuotojų sąmoningumu ugdymu bei mokymu;

14.4. dalyvauja atliekant poveikio duomenų apsaugai vertinimus NBFC;

14.5. atlieka kontaktinio asmens funkcijas, kai asmenys į NBFC kreipiasi su asmens duomenų tvarkymu susijusiais klausimais ir Valstybinei duomenų apsaugos inspekcijai kreipiantis į NBFC su asmens duomenų tvarkymu susijusiais klausimais;

14.6. rengia šias Taisykles, visas kitas su asmens duomenų apsauga susijusias vidaus taisykles, procedūras, prižiūri, kaip jų laikomasi;

14.7. rengia su asmens duomenų apsauga susijusių dokumentų blankus, dokumentus ir bent vieną kartą per metus juos peržiūri;

14.8. praneša apie esamus ar galimus Reglamento ir duomenų apsaugos įstatymų pažeidimus, keliančius pavojų NBFC veiklai, vadovybei, bei konsultuoja darbuotojus, atsakingus už šių pažeidimų ar jų grėsmės pašalinimą;

14.9. praneša NBFC vadovybei, kai nesivadovaujama duomenų apsaugos pareigūno nuomone;

14.10. atlieka asmens duomenų saugumo pažeidimų valdymą bei duomenų subjektų teisių įgyvendinimo valdymą.

V SKYRIUS DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

15. NBFC renka, naudoja ir saugo asmens duomenis pagal duomenų tvarkymo veiklos įrašus. Darbuotojai turi rinkti, naudoti ir saugoti duomenis tokia apimtimi, kuri nurodyta duomenų tvarkymo veiklos įrašuose.

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

17. Gavęs Taisyklių 16 punkte apibūdintą darbuotojo pranešimą, duomenų apsaugos pareigūnas turi nustatyti, ar pranešime nurodytas asmens duomenų rinkimas, naudojimas ir (arba) saugojimas atitinka Reglamentą bei kitus duomenų apsaugos įstatymus, ir, jei reikia, atnaujinti duomenų tvarkymo veiklos įrašus.

18. Duomenų tvarkymo veiklos įrašai tvarkomi raštu, įskaitant ir elektroninę formą, pagal šių Taisyklių 1 ir 2 prieduose pateiktas formas.

19. Duomenų tvarkymo veiklos įrašus rengia ir, esant poreikiui, pildo duomenų apsaugos pareigūnas, remdamasis informacija, kurią jam teikia darbuotojai (struktūriniai padaliniai), atsakingi už atitinkamų asmens duomenų tvarkymą. Darbuotojai (struktūriniai padaliniai), atsakingi už atitinkamų asmens duomenų tvarkymą, nedelsdami informuoja duomenų apsaugos pareigūną apie pasikeitimus, atsiradusius tvarkant atitinkamus asmens duomenis.

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

VI SKYRIUS POVEIKIO ASMENS DUOMENŲ APSAUGAI VERTINIMAS

21. Tuo atveju, jei pirmą kartą NBFC ketinama kurti, diegti ar naudoti tam tikras informacines ir ryšių technologijas ir (arba) kitus metodus, skirtus rinkti, naudoti ar saugoti asmens duomenis, atsakingas darbuotojas turi prieš protingą terminą apie tai informuoti duomenų apsaugos pareigūną.

22. Duomenų apsaugos pareigūnas stebi NBFC veiklą siekdamas nustatyti, ar tam tikros informacinės ir ryšių technologijos ir (arba) kiti metodai bus kuriami, diegiami ar naudojami siekiant rinkti, naudoti ar saugoti asmens duomenis.

23. Gavęs Taisyklių 21 punkte įvardytą darbuotojo pranešimą ar nustatęs, kad bet kurios konkrečios informacinės ir ryšių technologijos bus kuriamos, diegiamos ar naudojamos asmens duomenims rinkti, duomenų apsaugos pareigūnas turi nedelsdamas suteikti raštišką konsultaciją atsakingam (-iems) darbuotojui (-ams) ar atlikti poveikio duomenų apsaugai vertinimą.

24. Duomenų apsaugos pareigūnas teikia konsultacijas atsakingam (-iems) darbuotojui (-ams) dėl poreikio atlikti poveikio duomenų apsaugai vertinimą tais atvejais, kai siekiant rinkti, naudoti ar saugoti duomenis NBFC bus kuriamos, diegiamos ar naudojamos arba iš esmės duomenų rinkimo, naudojimo ar saugojimo požiūriu keičiamos informacinės ir ryšių technologijos ir (arba) metodai.

25. Vertinant, ar turi būti atliekamas poveikio asmens duomenų apsaugai vertinimas, privalo būti atsižvelgiama į Valstybinės duomenų apsaugos inspekcijos paskelbtus sąrašus, kuriuose

nurodytos duomenų tvarkymo operacijos, kurioms taikomas reikalavimas atlikti poveikio asmens duomenų apsaugai vertinimą.

26. Atsakingas darbuotojas turi atlikti poveikio duomenų apsaugai vertinimą užpildydamas poveikio duomenų apsaugai vertinimo formą (3 priedas) dėl kiekvienos konkrečios informacinės ir ryšių technologijos ir (ar) metodo, skirto rinkti, naudoti ar saugoti duomenis, ir laikydamasis Reglamento, duomenų apsaugos įstatymų bei šių Taisyklių reikalavimų.

27. Užpildytoje poveikio duomenų apsaugai vertinimo formoje privalo būti pateikta duomenų apsaugos pareigūno nuomonė dėl asmens duomenų tvarkymo teisėtumo, planuojamų priemonių pavojams mažinti ar pašalinti bei dėl galimybės toliau tvarkyti asmens duomenis.

VII SKYRIUS

IŠANKSTINĖS KONSULTACIJOS SU VALSTYBINE DUOMENŲ APSAUGOS INSPEKCIJA IR PAKLAUSIMŲ VALDYMAS

28. Jeigu, atlikus poveikio asmens duomenų apsaugai vertinimą, buvo nustatyta, kad NBFC 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 dėl išankstinės konsultacijos. Išankstinių konsultacijų metu Valstybinė duomenų apsaugos inspekcija gali teikti papildomas rekomendacijas.

29. Duomenų apsaugos pareigūnas bendradarbiauja su Valstybine duomenų apsaugos inspekcija, analizuoja ir atsako į jos paklausimus, inspekcijos prašymu renka informaciją, jei reikia, prašo paslaugų teikėjų ir trečiųjų asmenų pagalbos arba kreipiasi į inspekciją su prašymu suteikti raštišką konsultaciją.

30. Duomenų apsaugos pareigūnas NBFC atlieka Valstybinės duomenų apsaugos inspekcijos paklausimų valdymą vadovaudamasis Reglamentu, duomenų apsaugos įstatymais ir šiomis Taisyklėmis.

31. Duomenų apsaugos pareigūnas stebi NBFC veiklą, siekdamas nustatyti, ar buvo gauta bet kokių Valstybinės duomenų apsaugos inspekcijos paklausimų:

31.1. NBFC darbuotojas, gavęs Valstybinės duomenų apsaugos inspekcijos paklausimą, nedelsdamas, bet ne vėliau kaip per 1 (vieną) darbo dieną, informuoja duomenų apsaugos pareigūną apie gautą paklausimą.

31.2. Duomenų apsaugos pareigūnas, gavęs informaciją iš darbuotojo, kaip nurodyta Taisyklių 31.1 punkte, apie gautą paklausimą arba apie tai sužinojęs pats, turi nedelsdamas atlikti pirminę inspekcijos paklausimo analizę remdamasis šių Taisyklių 31.3. punktu.

31.3. Atlikdamas pirminę Valstybinės duomenų apsaugos inspekcijos paklausimo analizę, duomenų apsaugos pareigūnas turi:

31.3.1. peržiūrėti Valstybinės duomenų apsaugos inspekcijos paklausimą;

31.3.2. nustatyti atsakymo į inspekcijos paklausimą terminus (įskaitant reikalingos informacijos surinkimą, konsultacijas su darbuotojais ir (arba) paslaugų teikėjais) ir patikslinti šiame skyriuje nurodytus terminus, jei to reikia, kad būtų laikomasi inspekcijos nustatytų terminų;

31.3.3. kreiptis į inspekciją dėl termino pateikti atsakymą pratęsimo, jeigu to reikia;

31.3.4. nustatyti, ar yra reikalinga papildoma informacija iš darbuotojų, ir, jeigu reikia, paprašyti tokią informaciją pateikti;

31.3.5. nustatyti, ar reikia papildomos informacijos iš paslaugų teikėjų ir (arba) trečiųjų šalių, ir, jeigu reikia, paprašyti tokią informaciją pateikti.

VIII SKYRIUS

PASLAUGŲ TEIKĖJAI

32. Prieš pirmą sykį NBFC pasitelkiant tam tikrą paslaugų teikėją, darbuotojai turi iš anksto apie tai informuoti duomenų apsaugos pareigūną ir gauti jo konsultaciją.

33. Duomenų apsaugos pareigūnas turi pasirūpinti, kad NBFC, prieš dalydamasis duomenimis su paslaugų teikėju, sudarytų su juo duomenų tvarkymo sutartį (arba įtrauktų atitinkamas nuostatas į esamas sutartis, įskaitant paslaugų teikimo sąlygas bei atitinkamas Reglamento ir duomenų apsaugos įstatymų nuostatas).

34. Tais atvejais, kai paslaugų teikėjas pateikia NBFC savo duomenų tvarkymo sutarties formą, įskaitant paslaugų teikimo sąlygas, duomenų apsaugos pareigūnas, prieš NBFC sudarant tokią sutartį, turi įsitikinti, kad ji atitinka Reglamentą ir duomenų apsaugos įstatymų nustatytus reikalavimus, ir suteikti atsakingiems darbuotojams atitinkamą konsultaciją.

35. Duomenų apsaugos pareigūnas pasirūpina, kad visi paslaugų teikėjai būtų įtraukti į NBFC duomenų tvarkymo veiklos įrašus.

IX SKYRIUS BAIGIAMOSIOS NUOSTATOS

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

37. NBFC darbuotojai, pažeidę šias Taisykles, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

38. Šios Taisyklės turi būti pateiktos visiems NBFC darbuotojams susipažinti ir patvirtinti raštu, įskaitant elektroninę formą dokumentų valdymo sistemoje „Avilys“, apie susipažinimą su Taisyklėmis.

Nacionalinio bendrųjų funkcijų centro asmens duomenų tvarkymo taisyklių 1 priedas

(Duomenų valdytojo duomenų tvarkymo veiklos įrašo forma)

Duomenų valdytojas			
Duomenų valdytojo (jei taikoma, ir bendro duomenų valdytojo) pavadinimas (jei fizinis asmuo – vardas ir pavardė)			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės (pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)
Duomenų apsaugos pareigūnas			
Duomenų apsaugos pareigūno vardas ir pavardė			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės
Duomenų tvarkymo tikslas (pvz., įdarbinimas, prekių ir (ar) paslaugų pardavimas, tiesioginė rinkodara, personalo administravimas, turto saugumo užtikrinimas (kai vykdomas vaizdo stebėjimas), paslaugų kokybės užtikrinimas (kai įrašomi telefoniniai pokalbiai) ir t. t.)			
Duomenų subjektų kategorijų aprašymas (pvz., darbuotojai, asmenys, patenkantys į vaizdo stebėjimo lauką, pirkėjai, klientai, mokiniai, pacientų įgalioti atstovai ir t. t.) Esant kelioms duomenų subjektų grupėms, atskirai nurodomi kiekvienos duomenų subjektų grupės tvarkomi asmens duomenys (įskaitant ir specialiųjų kategorijų asmens duomenis), jeigu tvarkomi duomenys yra skirtingi.			
Asmens duomenų kategorijų aprašymas (pvz., vardas, pavardė, gimimo data, adresas, vaizdo duomenys, apskaičiuotas darbo užmokestis, duomenys apie sveikatą, telefoninio pokalbio įrašas, IP adresas ir t. t.)			

<p>Duomenų gavėjų kategorijos (duomenų gavėjai, kuriems buvo arba bus atskleisti ar kitaip perduoti asmens duomenys, įskaitant duomenų gavėjus trečiojoje valstybėje ar tarptautines organizacijas)</p> <p><i>(pvz., draudimo bendrovės, kurjerių tarnybos, bankai ir t. t.)</i></p>	
<p>Asmens duomenų perdavimas į trečiąją valstybę arba tarptautinei organizacijai (kai taikoma)</p>	
<p>Trečiojo valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys, pavadinimas</p>	<p>BDAR 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimo atvejais tinkamų apsaugos priemonių dokumentai</p>
<p>Kita informacija, susijusi su asmens duomenų perdavimu</p>	
<p>Numatomi asmens duomenų saugojimo, ištrynimo terminai (kai įmanoma) <i>(pvz., 10 metų po sutarties įvykdymo, 30 kalendorinių dienų, 1 metai nuo paskutinio prisijungimo prie kliento paskyros ir t. t.)</i></p>	
<p>Bendras duomenų saugumo priemonių (nurodytų BDAR 32 straipsnio 1 dalyje) aprašymas (kai įmanoma)</p>	
<p>Techninės saugumo priemonės</p> <p><i>(pvz., programinė įranga yra nuolat atnaujinama, aprūpinta ugniasienėmis ir antivirusinėmis programomis, daromos atsarginės duomenų kopijos, atliekamas duomenų šifravimas ir t. t.)</i></p>	<p>Organizacinės saugumo priemonės</p> <p><i>(pvz., informacinių sistemų ir duomenų bazių vartotojų teisių ribojimas ir kontrolė, asmenys, dirbantys su asmens duomenimis, yra saistomi teisės aktuose nustatytų konfidencialumo pareigų ir t. t.)</i></p>
<p>Kita informacija <i>(pvz., duomenų šaltiniai, duomenų tvarkymo teisiniai pagrindai, darbuotojai (skyriai), atsakingi už duomenų tvarkymą, duomenų subjekto teisių įgyvendinimo ypatumai, nuorodos į kitus su duomenų apsauga susijusius dokumentus (į poveikio duomenų apsaugai vertinimą, vidaus tvarkos taisykles ir t. t.)</i></p>	
<p>Duomenų įvedimo, keitimo data (-os)</p>	

Nacionalinio bendrųjų funkcijų centro asmens duomenų tvarkymo taisyklių 2 priedas

(Duomenų tvarkytojo duomenų tvarkymo veiklos įrašo forma)

Duomenų tvarkytojas			
Duomenų tvarkytojo pavadinimas (jei fizinis asmuo – vardas ir pavardė)			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės <i>(pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)</i>
Kiekvienas duomenų valdytojas (jei taikoma – ir jo atstovas), kurio vardu veikia duomenų tvarkytojas			
Duomenų valdytojo pavadinimas (jei fizinis asmuo – jo vardas ir pavardė)			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės <i>(pvz., interneto svetainės adresas, el. siuntos pristatymo dėžutės adresas)</i>
Duomenų apsaugos pareigūnas (jei taikoma)			
Duomenų apsaugos pareigūno vardas ir pavardė			
Pašto adresas	Telefono ryšio numeris	Elektroninio pašto adresas	Kitos ryšių priemonės
Kiekvieno duomenų valdytojo vardu atliekamo duomenų tvarkymo kategorijos, t. y. atliekami asmens duomenų tvarkymo veiksmai (pvz., vaizdo stebėjimas, asmens duomenų saugojimas, naikinimas ir t. t.)			
Asmens duomenų perdavimai į trečiąją valstybę arba tarptautinei organizacijai (kai taikoma)			
Trečiosios valstybės arba tarptautinės organizacijos, kuriai perduodami asmens duomenys, pavadinimas		BDAR 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimo atvejais tinkamų apsaugos priemonių dokumentai	
Kita informacija, susijusi su asmens duomenų perdavimu			

Bendras duomenų saugumo priemonių (nurodytų BDAR 32 straipsnio 1 dalyje) aprašymas (kai įmanoma)	
Techninės saugumo priemonės <i>(pvz., programinė įranga yra nuolatos atnaujinama, aprūpinta ugniasienėmis ir antivirusinėmis programomis, daromos atsarginės duomenų kopijos, atliekamas duomenų šifravimas ir t. t.)</i>	Organizacinės saugumo priemonės <i>(pvz., informacinių sistemų ir duomenų bazių vartotojų teisių ribojimas ir kontrolė, asmenys, dirbantys su asmens duomenimis, yra saistomi teisės aktuose nustatytų konfidencialumo pareigų ir t. t.)</i>
Kita informacija <i>(pvz., darbuotojai (skyriai), atsakingi už duomenų tvarkymą, nuorodos į kitus su duomenų apsauga susijusius dokumentus ir t. t.)</i>	
Duomenų įvedimo, keitimo data (-os)	

Nacionalinio bendrųjų funkcijų centro
asmens duomenų tvarkymo taisyklių
3 priedas

(Poveikio duomenų apsaugai vertinimo forma)

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

(Priemonės / metodo pavadinimas)

1. Priežastys, dėl kurių būtina atlikti poveikio duomenų apsaugai vertinimą

Planuojamos vykdyti veiklos aprašymas, jos tikslai ir planuojamos atlikti asmens duomenų tvarkymo operacijos. Paaiškinimas, kodėl būtina atlikti poveikio duomenų apsaugai vertinimą. Jei reikia, prie formos pridedami susiję dokumentai.

--

2. Asmens duomenų tvarkymo aprašymas

Aprašomi asmens duomenų rinkimo, naudojimo, saugojimo ir naikinimo veiksmai, nurodoma, iš kokių šaltinių bus renkami duomenys, kam bus teikiami (galima pateikti asmens duomenų tvarkymo veiksmų schemą). Aprašoma, kokie asmens duomenų tvarkymo veiksmai gali kelti pavojų fizinių asmenų teisėms ir laisvėms.

--

Aprašomas tvarkymo mastas: kokių kategorijų asmens duomenys bus tvarkomi; ar bus tvarkomi specialių kategorijų asmens duomenys arba duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas; kiek duomenų ir kaip dažnai bus renkama bei naudojama; kaip ilgai bus saugomi asmens duomenys; nurodomas apytikslis duomenų subjektų skaičius bei geografinė duomenų tvarkymo aprėptis.

--

Aprašomas duomenų tvarkymo pobūdis: kokio pobūdžio santykiai sieja Jūsų įmonę su duomenų subjektais; ar duomenų subjektai turės galimybę kontroliuoti duomenų tvarkymą; ar duomenų subjektai gali numatyti, kad jų asmens duomenys bus tvarkomi šiuo būdu; ar bus tvarkomi vaikų ir kitų pažeidžiamų asmenų duomenys; įvertinama, ar toks duomenų tvarkymas yra saugus; ar duomenų tvarkymo technologijos yra naujos, ar egzistuojančios technologijos bus panaudotos kitokiu būdu; koks yra technologijų išsivystymo lygis šioje srityje; ar yra kokių nors visuomeninių ar pan. problemų ar klausimų, į kuriuos būtina atsižvelgti; nurodoma, ar yra įsipareigojimas laikytis patvirtinto elgesio kodekso ar patvirtinto sertifikavimo mechanizmo.

--

--

Aprašomi asmens duomenų tvarkymo tikslai: kokį rezultatą siekiama gauti; kokį poveikį tai turės fiziniams asmenims; kokia yra tokio duomenų tvarkymo nauda Jūsų įmonei bei kitiems asmenims.

--

3. Konsultacijos

Aprašoma, kaip planuojama sužinoti suinteresuotų asmenų nuomonę, arba pagrindžiama, kodėl to daryti nebūtina: kokių asmenų nuomonę planuojama gauti; kokie asmenys bus pasitelkti Jūsų įmonėje, ar bus pasitelkti duomenų tvarkytojai; ar planuojama konsultuotis su duomenų saugos ekspertais ar kitų sričių ekspertais.

--

4. Būtinumo ir proporcingumo įvertinimas

Aprašomas asmens duomenų tvarkymo teisėtumas ir tvarkymo proporcingumas: nurodomas teisėto tvarkymo pagrindas; įvertinama, ar tvarkant asmens duomenis bus pasiektas Jūsų tikslas; ar tą patį rezultatą įmanoma pasiekti kitokiu būdu; koku būdu bus išvengta veiklos sutrikimų; kaip bus užtikrinta duomenų kokybė ir įgyvendintas duomenų kiekio mažinimo principas; kokia informacija bus pateikta duomenų subjektams; kaip Jūsų įmonė planuoja įgyvendinti duomenų subjektų teises; koku būdu bus užtikrinta, kad duomenų tvarkytojas laikytųsi reikalavimų; koku būdu bus užtikrintas į užsienio valstybes teikiamų asmens duomenų saugumas.

--

5. Pavojų nustatymas ir įvertinimas

Aprašomas pavojaus ir poveikio fiziniam asmeniui pobūdis. Jei būtina, aprašoma susijusi verslo rizika.	Žalos tikimybė	Žalos sunkumas	Bendras pavojaus lygis
	Mažai tikėtina, tikėtina ar labai tikėtina	Minimali, reikšminga ar sunki	Žemas, vidutinis ar aukštas

6. Priemonių pavojui sumažinti nustatymas

Nurodomos papildomos priemonės, kurių galima imtis siekiant sumažinti ar panaikinti aukšto ar vidutinio lygio pavojų.

Pavojus	Priemonės pavojui sumažinti ar pašalinti	Priemonės pritaikymo rezultatas	Likęs pavojus	Priemonė patvirtinta
		Pašalinta, sumažinta, priimtina rizika	Žemas, vidutinis ar aukštas	Taip, ne

7. Išvados ir sprendimai

Nurodomos priemonės ir įvardijamas likęs pavojus	Vardas, pavardė, data, parašas	Pastabos
Priemonės patvirtintos		Įtraukti numatytas priemones į veiklos planą, nustatant atlikimo terminą ir atsakingus asmenis
Likęs pavojus pripažintas priimtina rizika		Jei priimtina rizika pripažintas aukšto lygio pavojus priimtinas, privaloma kreiptis dėl išankstinės konsultacijos į Valstybinę duomenų apsaugos inspekciją

Duomenų apsaugos pareigūno nuomonė

Duomenų apsaugos pareigūnas pateikia nuomonę dėl asmens duomenų tvarkymo teisėtumo, planuojamų priemonių pavojams mažinti ar pašalinti bei dėl galimybės toliau tvarkyti asmens duomenis.

Pateikiama duomenų apsaugos pareigūno nuomonė	
	<i>Vardas, pavardė, data, parašas</i>

Nurodoma, ar atsižvelgta į duomenų apsaugos pareigūno nuomonę

Jeigu atmesta, pagrindžiama, kodėl

	<i>Vardas, pavardė, data, parašas</i>
--	---------------------------------------

Gauta kitų asmenų nuomonė

Trumpai aprašoma kitų asmenų nuomonė ir nurodoma, ar į ją atsižvelgta. Jeigu sprendimas skiriasi nuo susijusių asmenų nuomonės, pagrindžiama, kodėl.
--

	<i>Vardas, pavardė, data, parašas</i>
--	---------------------------------------

Už poveikio duomenų apsaugai vertinimo priežiūrą paskirtas atsakingas asmuo

Pastaba. Duomenų apsaugos pareigūnas turi prižiūrėti, ar asmens duomenys tvarkomi atsižvelgiant į Poveikio duomenų apsaugai vertinime nurodytas išvadas ir sprendimus.

	<i>Vardas, pavardė, data, parašas</i>
--	---------------------------------------

Nacionalinio bendrųjų funkcijų centro
asmens duomenų tvarkymo taisyklių 4
priedas

ORGANIZACINIŲ IR TECHNINIŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ APRAŠAS

Siekiant apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, nuo bet kokio kito neteisėto tvarkymo, Nacionaliniame bendrųjų funkcijų centre yra taikomos toliau išdėstytos organizacinės ir techninės duomenų saugumo priemonės:

1. Užtikrinama prieigos prie asmens duomenų apsauga, valdymas ir kontrolė. Prieiga prie asmens duomenų suteikiama tik tam darbuotojui, kuriam asmens duomenys yra reikalingi jo darbo funkcijoms vykdyti. Darbo santykiams pasibaigus, prieigos buvusiam darbuotojui panaikinamos.

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

3. Užtikrinama asmens duomenų apsauga nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis. Vidinis tinklas yra apsaugotas ugniasienėmis, taip pat naudojamos ryšio ir tinklo srautų atakų prevencijos priemonės.

4. Užtikrinama, kad visi su asmens duomenų tvarkymu susiję darbuotojai būtų įsipareigoję neatskleisti asmens duomenų kita, ne teisės aktuose, reglamentuojančiuose asmens duomenų apsaugą, nustatyta tvarka. Šiam tikslui pasiekti Centro darbuotojai pasirašo įsipareigojimus dėl asmens duomenų tvarkymo.

5. Kiekvienam darbuotojui, kuriam suteikta prieiga prie asmens duomenų, tvarkomų automatinio būdu, suteikiamas unikalus prisijungimo vardas ir vienkartinis slaptažodis, kurį pirmo prisijungimo metu privalu pasikeisti į nuolatinį slaptažodį. Nuolatinis slaptažodis negali būti trumpesnis nei 8 simboliai ir negali būti sudaromas naudojant asmeninio pobūdžio informaciją. Slaptažodis keičiamas ne rečiau kaip kartą per 3 (tris) mėnesius. Tas pats slaptažodis negali būti kartojamas kelis kartus. Darbuotojas yra atsakingas už slaptažodžio konfidencialumą ir įsipareigoja neatskleisti jo tretiesiems asmenims.

6. Nacionalinio bendrųjų funkcijų centro patalpos rakinamos. Į Nacionalinio bendrųjų funkcijų centro patalpas, kuriose yra tvarkomi asmens duomenys, patenka tik įgalioti asmenys. Įgalioti asmenys, kurie nėra Nacionalinio bendrųjų funkcijų centro darbuotojai, ir klientai į nurodytas patalpas patenka tik kartu su įgaliotu Nacionalinio bendrųjų funkcijų centro darbuotoju.

7. Naudojama tik legali ir leistina programinė įranga. Nuolat atliekama kompiuterinėse darbo vietose naudojamos programinės įrangos kontrolė.

8. Užtikrinamas tinkamas techninės įrangos išdėstymas ir priežiūra, informacinių sistemų priežiūra, tinklo valdymas, naudojimosi internetu saugumas, kompiuterinės įrangos apsauga nuo kenksmingos programinės įrangos (diegiamos ir atnaujinamos antivirusinės programos). Už šių priemonių įgyvendinimą ir priežiūrą atsako Nacionalinio bendrųjų funkcijų centro Veiklos skaitmeninio grupė ir informacinių technologijų paslaugas pagal sutartį teikianti įmonė.

9. Darbuotojų kompiuteriuose tvarkoma informacija, susijusi su asmens duomenimis, yra neperteklinė, būtina tik kasdienėms darbo funkcijoms atlikti. Informacija, kuri nebėra aktuali ir reikalinga darbo funkcijoms atlikti, periodiškai (kas mėnesį) ištrinama.

10. Jei darbuotojas abejoja įdiegtų saugumo priemonių patikimumu, jis privalo kreiptis į vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir įdiegimas.

11. Įvykus gedimui, asmens duomenys, esantys serveryje, atkuriami iš atsarginių kopijų. Duomenų serverio atsarginės kopijos daromos kartą per 24 valandas.

12. Visuose serveriuose įdiegta antivirusinė programa bei įrengta ugniasienė. Duomenų bazės apsaugotos vartotojų slaptažodžiais. Prisijungimai galimi tik iš nurodytų vartotojų IP adresų.

13. Asmens duomenų saugumo pažeidimų valdymo tvarkos apraše detaliai reglamentuota asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarka Nacionaliniame bendrųjų funkcijų centre.

14. Įvykus duomenų saugumo incidentui, apie duomenų saugumo incidentus ir saugumo priemones, kurių imtasi siekiant apsaugoti asmens duomenis, nedelsiant informuojamas duomenų apsaugos pareigūnas.
