

KRAŠTO APSAUGOS MINISTERIJOS BENDRŪJŲ REIKALŲ DEPARTAMENTO ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Krašto apsaugos ministerijos bendrųjų reikalų departamento asmens duomenų tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja asmens duomenų tvarkymo reikalavimus, duomenų subjektų teisių įgyvendinimo tvarką, asmens duomenų saugumo pažeidimų valdymą Krašto apsaugos ministerijos bendrųjų reikalų departamente (toliau – KAMBRD), KAMBRD darbuotojų kompetenciją, atsakomybę bei teises ir pareigas asmens duomenų tvarkymo srityje.

2. Asmens duomenys KAMBRD tvarkomi vadovaujantis:

2.1. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu (toliau – Asmens duomenų, tvarkomų teisės saugos ar nacionalinio saugumo tikslais, įstatymas), Lietuvos Respublikos krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymu, Lietuvos Respublikos kariuomenės drausmės statutu, Lietuvos Respublikos karių materialinės atsakomybės įstatymu, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu ir kitais teisės aktais, kurie numato, kad asmens duomenys tvarkomi vadovaujantis Asmens duomenų, tvarkomų teisės saugos ar nacionalinio saugumo tikslais, įstatymu – kai asmens duomenys tvarkomi nacionalinio saugumo ir gynybos tikslais;

2.2. 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 (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – ADTAĮ), kitais teisės aktais, kai pagal juos asmens duomenys tvarkomi vadovaujantis Reglamentu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu – kai asmens duomenys tvarkomi kitais tikslais;

2.3. Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto apsaugos sistemoje taisyklėmis (toliau – KAS asmens duomenų tvarkymo taisyklės), patvirtintomis Lietuvos Respublikos krašto apsaugos ministro 2015 m. gruodžio 3 d. įsakymu Nr. V-1253;

2.4. Taisyklėmis ir kitais KAMBRD priimtais teisės aktais;

2.5. Lietuvos Respublikos darbo kodekso 27 straipsnio 1 dalimi, Valstybinės duomenų apsaugos inspekcijos priimtais teisės aktais, rekomendacijomis, gairėmis.

3. Taisyklių privalo laikytis visi KAMBRD tarnaujantys kariai, darbuotojai, dirbantys pagal darbo sutartis, asmenys, priimti atlikti praktiką KAMBRD (toliau visi kartu – darbuotojai), kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

II SKYRIUS ASMENS DUOMENŲ TVARKYMAS

4. KAMBRD asmens duomenys yra tvarkomi vadovaujantis Reglamento 5 straipsnio 1 dalyje nustatytais teisėtumo, sąžiningumo ir skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo principais, taip pat Asmens duomenų, tvarkomų teisės saugos ar nacionalinio saugumo tikslais, įstatymo 3 straipsnyje numatytais asmens duomenų tvarkymo principais.

5. Asmens duomenys gali būti tvarkomi tik tuo tikslu, kuriuo yra renkami. Jeigu asmens duomenys nėra būtini tam, kad būtų pasiektas konkretus tikslas, jie negali būti tvarkomi. Konkrečiam tikslui pasiekti yra tvarkomas kiek įmanoma mažesnis kiekis asmens duomenų. Asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, turi būti nedelsiant ištrinami arba ištaisomi – KAMBRD imamasi visų pagrįstų priemonių užtikrinti, kad būtų laikomasi Taisyklių 4 punkte nustatytų principų.

6. KAMBRD, kaip duomenų valdytojo, pagrindiniai asmens duomenų tvarkymo tikslai, duomenų apimtis ir duomenų subjektai nurodomi šių Taisyklių priede. Vadovaujantis Reglamentu ir ADTAĮ, tvarkomų asmens duomenų tvarkymo tikslai, asmens duomenų kategorijos ir duomenų subjektai nurodyti priedo II skyriuje, nacionalinio saugumo ir gynybos tikslais tvarkomų asmens duomenų kategorijos, tikslai, duomenų subjektai nurodyti priedo I skyriuje.

7. KAMBRD gali būti tvarkomi ir Taisyklių priede nenurodyti asmens duomenys, tačiau nurodyti KAMBRD veiklai taikomuose teisės aktuose ir (ar) KAMBRD su kitais duomenų valdytojais sudarytuose duomenų tvarkymo susitarimuose.

8. KAMBRD tvarkomi konkretūs asmens duomenys, jų tvarkymo tikslai, saugojimo terminai bei tvarkymo teisiniai pagrindai pateikiami KAMBRD, kaip duomenų valdytojo, tvarkomuose duomenų tvarkymo veiklos įrašuose, rengiamuose šių Taisyklių VII skyriaus nustatyta tvarka.

9. Asmens duomenys tvarkomi automatinio ir neautomatinio būdu, automatiniai sprendimai nepriimami, profiliavimas netaikomas.

10. Specialių kategorijų asmens duomenys KAMBRD tvarkomi tik esant Reglamento 9 straipsnyje nurodytiems pagrindams (kai asmens duomenys tvarkomi vadovaujantis Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais, įstatymu – esant šio įstatymo 8 straipsnyje nurodytam pagrindui) ir laikantis kitų teisės aktų nustatytų sąlygų. Specialių kategorijų asmens duomenys neteikiami jokiems duomenų gavėjams ar kitiems tretiesiems asmenims, išskyrus atvejus, kai tam yra teisinis pagrindas.

11. Tais atvejais, kai asmens duomenų tvarkymo KAMBRD pagrindas yra duomenų subjekto sutikimas, KAMBRD darbuotojai sutikimo iš duomenų subjekto prašo raštu ar elektroninėmis priemonėmis, sutikimo turinį aiškiai atskirdami nuo kitų klausimų, pateikdami suprantama ir lengvai prieinama forma, taip pat paaiškindami subjektui, kokių tikslu bus tvarkomi jo asmens duomenys, ir pateikdami kitą svarbią informaciją, kartu informuoja duomenų subjektą apie teisę bet kuriuo metu atšaukti sutikimą ir kaip jis atšaukiamas. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui.

III SKYRIUS DUOMENŲ APSAUGOS PAREIGŪNAS

12. KAMBRD duomenų apsaugos pareigūnas – KAMBRD direktoriaus įsakymu paskirtas asmuo, turintis Reglamente, Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais, įstatyme, KAS asmens duomenų tvarkymo taisyklėse ir šiose Taisyklėse nustatytas teises ir pareigas.

13. KAMBRD duomenų apsaugos pareigūnas:

13.1. informuoja darbuotojus apie jų pareigas, nustatytas asmens duomenų apsaugą reglamentuojančiuose teisės aktuose, ir juos konsultuoja šiais klausimais;

13.2. stebi ir analizuoja, ar asmens duomenys yra tvarkomi pagal Taisyklių ir kitų teisės aktų, reglamentuojančių asmens duomenų tvarkymą, reikalavimus, ir teikia Krašto apsaugos ministerijos (toliau – KAM) duomenų apsaugos pareigūnui pasiūlymus dėl asmens duomenų apsaugos tobulinimo;

13.3. vykdo KAMBRD duomenų saugumo pažeidimų apskaitą;

13.4. teikia KAMBRD vadovui ar įgaliotam asmeniui pasiūlymus dėl priemonių asmens duomenų saugumo pažeidimo pasekmėms sumažinti ar pašalinti, Reglamento 33 ir 34 straipsniuose nustatytais atvejais nedelsdamas teikia KAM duomenų apsaugos pareigūnui reikalingą informaciją dėl pranešimų apie asmens duomenų saugumo pažeidimus Valstybinei duomenų apsaugos inspekcijai

ir duomenų subjektui. Įvykus KAM ar KAMBRD tvarkomų asmens duomenų saugumo pažeidimui, rūpinasi, kad būtų laiku ir tinkamai užpildyta Valstybinės duomenų apsaugos inspekcijos rekomenduojama Pranešimo apie asmens duomenų saugumo pažeidimo forma (toliau – Pranešimo forma) ir pateikta Valstybinei duomenų apsaugos inspekcijai. Įvykus KAMBRD duomenų saugumo pažeidimui, rūpinasi, kad būtų laiku įvykdytos Reglamente numatytos KAMBRD, kaip duomenų valdytojo ar kaip duomenų tvarkytojo, pareigos;

13.5. KAMBRD duomenų apsaugos pareigūnas yra atsakingas už duomenų veiklos įrašų pildymą;

13.6. teikia KAM duomenų apsaugos pareigūnui elektroniniu paštu asmens.duomenys@kam.lt informaciją, būtiną KAM, kaip duomenų valdytojos, asmens duomenų tvarkymo įrašams parengti ir atnaujinti;

13.7. vertina KAMBRD darbuotojų parengtų teisės aktų, reglamentuojančių asmens duomenų apsaugą ir jų tvarkymą, projektus, teikia dėl jų pastabas ir pasiūlymus;

13.8. savo iniciatyva, KAMBRD direktoriaus nurodymu ar KAM duomenų apsaugos pareigūno prašymu atlieka KAMBRD asmens duomenų, kurių valdytoja yra KAM, tvarkymo rizikos vertinimą, parengia ataskaitą, imasi priemonių rizikai pašalinti arba sumažinti, ataskaitą pateikia KAMBRD direktoriui, KAM kancleriui ir KAM duomenų apsaugos pareigūnui;

13.9. atlieka kitus teisės aktais jam numatytus atlikti veiksmus.

IV SKYRIUS DARBUOTOJŲ TEISĖS IR PAREIGOS

14. Darbuotojai tvarko asmens duomenis, vykdydami savo funkcijas teisės aktų nustatyta tvarka. Darbuotojas tvarko asmens duomenis, kol tokia funkcija jam priklauso pagal pareigas. Jei darbuotojas laikinai eina kito darbuotojo pareigas ar vykdo kito darbuotojo funkcijas, jis turi teisę tvarkyti asmens duomenis pareigų arba funkcijų vykdymo laikotarpiu.

15. Darbuotojas privalo:

15.1. saugoti asmens duomenų konfidencialumą visą tarnybos, darbo laiką ir pasibaigus tarnybos, darbo santykiams. Darbuotojas pasirašo pasižadėjimą (KAS asmens duomenų tvarkymo taisyklių 2 priedas) ir šis pasižadėjimas saugomas darbuotojo asmens byloje visą tarnybos, darbo laiką ir pasibaigus tarnybos, darbo santykiams asmens bylų saugojimo terminą;

15.2. saugoti asmens duomenų konfidencialumą visą tarnybos, darbo ar praktikos laiką ir pasibaigus tarnybos, darbo santykiams ar praktikai;

15.3. atlikti tik tuos asmens duomenų tvarkymo veiksmus, kuriuos atlikti yra teisinis pagrindas ar juos atlikti jam suteiktos teisės.

Jei darbuotojas pagal savo vykdomas funkcijas privalo ar gali suteikti prieigą prie KAMBRD tvarkomų popierinio formato dokumentų ar duomenų bei dokumentų KAMBRD ar krašto apsaugos sistemos (toliau – KAS) dokumentų valdymo ir kitose informacinėse sistemose, tais atvejais, kai dokumento ar duomenų turinys susijęs su asmens duomenimis ar informacija apie asmens gyvenimą, jis prieigą gali suteikti tik tiems darbuotojams, kuriems dokumentas skirtas ir (ar) reikalingas darbo / tarnybinėms funkcijoms ar užduotims atlikti (atsižvelgiant į principą „būtina žinoti“);

15.4. asmens duomenis tvarkyti tiksliai, nedelsdamas atnaujinti, ištaisyti ar papildyti netikslius, klaidingus, neišsamius asmens duomenis ir (ar) apriboti tokių asmens duomenų tvarkymą, išskyrus saugojimą;

15.5. asmens duomenis tvarkyti tik tokios apimties, kuri būtina jo funkcijoms atlikti;

15.6. asmens duomenis tvarkyti taip, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi;

15.7. dokumentus, kuriuose yra asmens duomenų (įsakymus, prašymus, raštus, sutartis ir kitus dokumentus, jų kopijas ar išrašus, taip pat asmens bylas, kompiuterines duomenų laikmenas su asmens duomenimis ir kt.), elektroniniu būdu tvarkyti tik darbuotojui suteiktomis darbo (kompiuterinėmis, programinėmis ir kitomis) priemonėmis;

15.8. neatlikti veiksmų, galinčių didinti duomenų saugumo pažeidimo riziką;

15.8.1. nesinešti į nuotolinio darbo vietas popierinio formato dokumentų, jų kopijų, išrašų, juodraščių su asmens duomenimis, išskyrus atvejus, kai tai būtina (tokiais atvejais pasirūpinti dokumentų saugumu);

15.8.2. atvirai nelaikyti dokumentų su asmens duomenimis, kad nebūtų sudaryta neteisėtos prieigos prie jų galimybė, nepalikti dokumentų su tvarkomais asmens duomenimis ar kompiuterio, kuriuo naudojantis galima atidaryti rinkmenas su asmens duomenimis, be priežiūros taip, kad juose esančią informaciją galėtų perskaityti ar kitaip panaudoti bet kurie kiti asmenys, neturintys teisės dirbti su tais asmens duomenimis;

15.8.3. netvarkyti asmens duomenų, jei yra rizika, kad toje pačioje patalpoje esantys kiti asmenys, neturintys teisės tvarkyti šių asmens duomenų ar jų tvarkyti tuo pačiu tikslu, gali juos matyti ar kitu būdu su jais susipažinti;

15.9. pastebėjęs galimą asmens duomenų saugumo pažeidimą, nedelsdamas atlikti Asmens duomenų saugumo pažeidimų valdymo tvarkos apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2019 m. liepos 12 d. įsakymu Nr. V-644 „Dėl Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo patvirtinimo“, nurodytus darbuotojui privalomus veiksmus, informuoti KAMBRD ir KAM duomenų apsaugos pareigūnus;

15.10. KAMBRD direktoriaus nurodymu ar leidimu pagal kompetenciją dalyvauti KAMBRD ir (ar) kitų institucijų rengiamuose asmens duomenų apsaugos mokymuose;

15.11. kylant neaiškumų dėl šių Taisyklių, Reglamento, ADTAĮ, Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais, įstatymo reikalavimų taikymo, vykdant paskirtas funkcijas, konsultuotis su KAMBRD duomenų apsaugos pareigūnu.

16. Darbuotojai, tvarkantys asmens duomenis ar organizuojantys jų tvarkymą, siekdami užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam duomenų tvarkymui, privalo konsultuotis su KAMBRD duomenų apsaugos pareigūnu, o kai klausimas susijęs su asmens duomenų, kurių valdytoja yra KAM, tvarkymu – taip pat ir su KAM duomenų apsaugos pareigūnu šiais klausimais:

16.1. nagrinėjant duomenų subjektų prašymus įgyvendinti jų teises pagal Taisykles ir teikiant informaciją duomenų subjektams;

16.2. tiriant duomenų saugumo pažeidimus;

16.3. rengiant norminio administracinio ar kito teisės akto projektą, jei jis susijęs su asmens duomenų tvarkymu ir (ar) apsauga;

16.4. rengiant informaciją apie duomenų tvarkymo veiklos įrašų pildymą, pakeitimą ar atnaujinimą;

16.5. sudarant, keičiant duomenų perdavimo (teikimo) sutartis, pagal kurias perduodami (teikiami) ir (ar) gaunami asmens duomenys, ar teikiant asmens duomenis pagal prašymą;

16.6. atliekant poveikio duomenų apsaugai vertinimą;

16.7. keičiant esamus ar nustatant naujus asmens duomenų tvarkymo procesus;

16.8. priimant sprendimus dėl asmens duomenų apsaugos priemonių, įskaitant technines ir organizacines, taikymo;

16.9. rengiant viešųjų pirkimų, kuriuos vykdant numatoma įsigyti asmens duomenų tvarkymo ir apsaugos priemonių (įskaitant technines ir organizacines), dokumentus.

17. KAMBRD darbuotojai turi bendradarbiauti su KAMBRD ir KAM duomenų apsaugos pareigūnais ir teikti jiems informaciją apie KAMBRD vykdomą asmens duomenų tvarkymą. KAMBRD duomenų apsaugos pareigūnas, taip pat darbuotojai bei asmenys, priimti atlikti praktiškai, turi bendradarbiauti su KAM duomenų apsaugos pareigūnu Taisyklių 16 punkte nurodytais atvejais, kai tai susiję su KAM, kaip duomenų valdytojos, tvarkomais asmens duomenimis.

18. Darbuotojams draudžiama be teisinio pagrindo tvarkyti asmens duomenis, juos naudoti asmeniniams, su vykdomomis darbo / tarnybinėmis funkcijomis nesusijusiems tikslams, daryti perteklines dokumentų kopijas, kurios nėra būtinos jų funkcijoms vykdyti.

Darbuotojams taip pat draudžiama skaityti, kopijuoti, saugoti, siųsti ir bet koku kitu būdu tvarkyti ar platinti KAS dokumentų valdymo ir kitose informacinėse sistemose, taip pat ir ne informacinėse sistemose esančius duomenis bei dokumentus, kurių valdytojas yra KAMBRD,

susijusius su konkrečiu asmeniu, jo gyvenimu bei veikla (tarnybinio tyrimo, tarnybinio nusižengimo ar drausmės pažeidimo tyrimo medžiagą bei išvadas, asmenų skundus, atsakymus į juos ir bet kuriuos kitus duomenis ar dokumentus, kai jų turinys atskleidžia asmens duomenis ar informaciją apie asmens gyvenimą, veiklą), kai tai nereikalinga tų darbuotojų darbo / tarnybinėms funkcijoms ar užduotims atlikti.

V SKYRIUS DUOMENŲ SUBJEKTO TEISĖS IR JŲ ĮGYVENDINIMO TVARKA

PIRMASIS SKIRSNIS DUOMENŲ SUBJEKTO TEISĖS

19. Kai KAMBRD asmens duomenys tvarkomi vadovaujantis Reglamentu, duomenų subjektai turi šias teises, įtvirtintas Reglamente:

19.1. teisę gauti informaciją apie savo asmens duomenų tvarkymą. Reglamento 13–14 straipsniuose nurodyta informacija apie asmens duomenų tvarkymą duomenų subjektams pateikiama:

19.1.1. šiose Taisyklėse, kituose teisės aktuose, reglamentuojančiuose asmens duomenų tvarkymą ir duomenų subjektų teisių įgyvendinimą. Apie naujai nustatomus duomenų tvarkymo tikslus ir tvarkomus asmens duomenis, jų tvarkymo pagrindą ir saugojimo terminus darbuotojai informuojami dokumentų valdymo sistemoje (DokVIS), esant reikalui, darbuotojai apie numatomą jų asmens duomenų tvarkymą taip pat gali būti informuojami tarnybiniu elektroniniu paštu, pateikiant jiems, kaip duomenų subjektams, reikiamą informaciją. Gavęs šią informaciją, darbuotojas turi su ja susipažinti ne vėliau kaip per 5 darbo dienas po jos pateikimo ar grįžimo į darbą;

19.1.2. įrengiant prieš įėjimą į patalpas ar jų dalį vaizdo stebėjimo informacines lenteles;

19.1.3. pateikiant informacinį pranešimą kompiuterio, kuriuo naudojasi duomenų subjektas, ekrane apie vaizdo įrašymą, retransliavimą;

19.2. teisę susipažinti su KAMBRD tvarkomais savo asmens duomenimis (duomenų subjektas turi teisę iš KAMBRD gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir Reglamento 15 straipsnyje nurodyta informacija);

19.3. teisę reikalauti, kad būtų ištaisyti netikslūs jo asmens duomenys ir (arba) papildyti neišsamūs jo asmens duomenys (duomenų subjektas turi teisę reikalauti, kad KAMBRD nepagrįstai nedelsdamas ištaisytų netikslus su juo susijusius asmens duomenis; atsižvelgdamas į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys);

19.4. teisę reikalauti ištrinti savo asmens duomenis (teisė būti pamirštam) (duomenų subjektas turi teisę reikalauti, kad nepagrįstai nedelsiant būtų ištrinami su juo susiję asmens duomenys, o KAMBRD yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis, jei tai galima pagrįsti viena iš Reglamento 17 straipsnio 1 dalyje nurodytų priežasčių; ši teisė gali būti neįgyvendinta Reglamento 17 straipsnio 3 dalyje numatytais atvejais);

19.5. teisę apriboti savo asmens duomenų tvarkymą (duomenų subjektas turi šią teisę Reglamento 18 straipsnio 1 dalyje numatytais atvejais);

19.6. teisę į savo asmens duomenų perkeliamumą (duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė KAMBRD susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui (neapsiribojant kitomis KAS institucijomis), o KAMBRD, kaip duomenų valdytojas, turi nesudaryti tam kliūčių, kai yra Reglamento 20 straipsnio 1 dalyje nurodytos aplinkybės (ši teisė netaikoma Reglamento 20 straipsnio 3 dalyje nurodytu atveju);

19.7. teisę nesutikti su savo asmens duomenų tvarkymu (duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi, kai toks duomenų tvarkymas vykdomas pagal Reglamento 6 straipsnio 1 dalies e arba f punktus, remiantis tomis nuostatomis, kaip tai numatyta Reglamento 21 straipsnyje);

19.8. teisę pateikti skundą Taisyklių 31 punkte nustatyta tvarka.

ANTRASIS SKIRSNIS DUOMENŲ SUBJEKTO TEISIŲ ĮGYVENDINIMAS

20. Duomenų subjektas, siekdamas įgyvendinti Taisyklių 19 punkte nurodytas teises asmeniškai, paštu ar per pasiuntinį arba elektroninių ryšių priemonėmis turi pateikti rašytinį (valstybine kalba) prašymą įgyvendinti duomenų subjekto teisę (-es).

21. Prašymas įgyvendinti duomenų subjekto teises turi būti aiškus, įskaitomas, paties asmens pasirašytas, jame turi būti nurodytas duomenų subjekto vardas, pavardė, kontaktiniai duomenys, kuriais asmuo pageidauja gauti atsakymą, informacija, kokią teisę ir kokios apimties duomenų subjektas pageidauja įgyvendinti.

22. Duomenų subjektas, pateikdamas prašymą, privalo patvirtinti savo tapatybę:

22.1. jei prašymas pateikiamas tiesiogiai, pateikdamas prašymą darbuotojui, registruojančiam prašymą, duomenų subjektas turi pateikti asmens tapatybę patvirtinantį dokumentą;

22.2. jei prašymas pateikiamas paštu, per pasiuntinį ar elektroniniu paštu, kartu su prašymu duomenų subjektas turi pateikti asmens tapatybę patvirtinančio dokumento kopiją ir (ar) kitu būdu patvirtinti savo tapatybę;

22.3. jei prašymas pateikiamas elektroninių ryšių priemonėmis, prašymą turi pasirašyti kvalifikuotu elektroniniu parašu arba prašymą suformuoti elektroninėmis priemonėmis, kurios leidžia užtikrinti teksto vientisumą ir nepakeičiamumą (pvz., informacinės sistemos „E. pristatymas“ atveju).

23. Duomenų subjektas savo teises gali įgyvendinti pats arba per įgaliotą atstovą.

24. Jeigu atstovaujamo duomenų subjekto vardu į KAMBRD kreipiasi duomenų subjekto atstovas, jis prašyme turi nurodyti savo vardą, pavardę, kontaktinius duomenis, kuriais asmens atstovas pageidauja gauti atsakymą, taip pat atstovaujamo asmens vardą, pavardę, informaciją, kokią duomenų subjekto teisę ir kokios apimties pageidauja įgyvendinti, ir pridėti atstovavimą patvirtinantį dokumentą ar jo kopiją, patvirtintą notaro arba kita teisės aktų nustatyta tvarka. Atstovo pateiktas prašymas turi atitikti Taisyklių 20–22 punktų reikalavimus.

25. Duomenų subjekto prašymas, pateiktas nesilaikant Taisyklių 20–24 punktuose nustatytų reikalavimų, nenagrinėjamas ir duomenų subjektas nedelsiant, bet ne vėliau kaip per 5 darbo dienas apie tai informuojamas nurodant prašymo nenagrinėjimo priežastis.

26. Gavus duomenų subjekto prašymą, ne vėliau kaip per vieną mėnesį nuo prašymo gavimo duomenų subjektui pateikiama informacija, kokių veiksmų buvo imtasi pagal gautą prašymą. Šis vieno mėnesio terminas prireikus gali būti pratęstas dar dviem mėnesiams (kai asmens duomenys tvarkomi vadovaujantis Reglamentu) arba trimis mėnesiams (kai asmens duomenys tvarkomi vadovaujantis Asmens duomenų, tvarkomų teisės saugos ar nacionalinio saugumo tikslais, įstatymu), atsižvelgiant į prašymų sudėtingumą ir jų skaičių. Kai duomenų subjektui neatsakoma per vieną mėnesį, KAMBRD per vieną mėnesį nuo duomenų subjekto prašymo gavimo raštu jam praneša apie termino pratęsimą ir nurodo vėlavimo (kai asmens duomenys tvarkomi vadovaujantis Reglamentu) ar pratęsimo (kai asmens duomenys tvarkomi vadovaujantis Asmens duomenų, tvarkomų teisės saugos ar nacionalinio saugumo tikslais, įstatymu) priežastis.

27. Nagrinėjant duomenų subjekto prašymą įvertinama, ar prašomos įgyvendinti duomenų subjekto teisės, vadovaujantis Reglamento 23 straipsniu ar Taisyklių 2 punkte nurodytais teisės aktais, neturėtų būti visiškai arba iš dalies apribotos įstatymų ir kitų teisės aktų nustatyta tvarka.

28. Informacija pagal duomenų subjekto prašymą dėl jo teisių įgyvendinimo pateikiama valstybine kalba. Kilus abejonių dėl duomenų subjekto tapatybės, atsakingas (tiek registruojantis prašymą, tiek jį nagrinėjantis) KAMBRD darbuotojas pareiškėjo gali paprašyti suteikti papildomos informacijos.

29. Jei pagal duomenų subjekto prašymą asmens duomenys yra ištaisomi, ištrinami ar jų tvarkymas yra apribojamas, prašymą išnagrinėjęs darbuotojas privalo apie tai informuoti kitus duomenų tvarkytojus, kuriems tokie duomenys buvo teikiami.

30. Visi veiksmai pagal duomenų subjekto prašymus įgyvendinti duomenų subjekto teises atliekami ir informacija teikiama nemokamai.

TREČIASIS SKIRSNIS SKUNDŲ PATEIKIMO TVARKA

31. KAMBRD, kaip duomenų valdytojo, veiksmus ar neveikimą, įgyvendinant duomenų subjekto teises, kai asmens duomenys tvarkomi vadovaujantis Reglamento nuostatomis, duomenų subjektas arba duomenų subjekto atstovas, taip pat jo įgaliota ne pelno įstaiga, organizacija ar asociacija, atitinkanti Reglamento 80 straipsnio reikalavimus, turi teisę skusti Valstybinei duomenų apsaugos inspekcijai (L. Sapiegos g. 17, Vilnius, el. p. ada@ada.lt, interneto svetainė <https://vdai.lrv.lt/>), taip pat Vilniaus apygardos administraciniam teismui, o tais atvejais, kai asmens duomenys tvarkomi nacionalinio saugumo ir gynybos tikslais (ar užtikrinant nacionalinį saugumą ir gynybą), – subjektui, kuris pagal Lietuvos Respublikos įstatymus, reglamentuojančius kompetentingų institucijų veiklą, nagrinėja skundus dėl žmogaus teisių ir laisvių pažeidimų, – Lietuvos Respublikos Seimo kontrolieriui (Gedimino pr. 56, Vilnius, el. p. ombuds@lrski.lt), taip pat Vilniaus apygardos administraciniam teismui (Žygimantų g. 2, Vilnius).

32. Prieš pateikiant skundą Valstybinei duomenų apsaugos inspekcijai, Lietuvos Respublikos Seimo kontrolieriui ar Vilniaus apygardos administraciniam teismui skundą dėl KAMBRD veiksmų ar neveikimo, įgyvendinant duomenų subjekto teises, duomenų subjektui siūloma kreiptis į KAMBRD direktorių.

KETVIRTASIS SKIRSNIS INFORMACIJOS DUOMENŲ SUBJEKTUI PATEIKIMAS

33. Kai KAMBRD asmens duomenys tvarkomi vadovaujantis Reglamentu:

33.1. kai duomenų subjekto asmens duomenys gauti iš duomenų subjekto, informacija apie KAMBRD atliekamą duomenų subjekto asmens duomenų tvarkymą, nurodyta Reglamento 13 straipsnyje, pateikiama, kai gaunami duomenų subjekto asmens duomenys, bendraujant su juo tokiu būdu, koku jis kreipėsi į KAMBRD. Informaciją raštu rekomenduojama teikti pagal KAS asmens duomenų tvarkymo taisyklių 5 priede pateiktą formą. Šis papunktis netaikomas, jeigu duomenų subjektas jau turi informaciją;

33.2. kai duomenų subjekto asmens duomenys renkami ne tiesiogiai iš duomenų subjekto, apie jo asmens duomenų tvarkymą duomenų subjektui pateikiama Reglamento 14 straipsnyje nurodyta informacija (informaciją rekomenduojama teikti pagal KAS asmens duomenų tvarkymo taisyklių 5 priede pateiktą formą):

33.2.1. per pagrįstą laikotarpį nuo asmens duomenų gavimo, bet ne vėliau kaip per vieną mėnesį, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes;

33.2.2. jeigu asmens duomenys bus naudojami ryšiams su duomenų subjektu palaikyti – ne vėliau kaip pirmą kartą susisiekus su tuo duomenų subjektu;

33.2.3. jeigu numatoma asmens duomenis atskleisti kitam duomenų gavėjui – ne vėliau kaip atskleidžiant duomenis pirmą kartą;

33.3. Taisyklių 33.2 papunktis netaikomas, kai duomenų subjektas tokią informaciją jau turi arba kai tokių duomenų rinkimo bei teikimo tvarka ir duomenų gavėjai apibrėžiami įstatymuose ir kituose teisės aktuose ar yra kitų Reglamento 14 straipsnio 5 dalyje nurodytų sąlygų;

33.4. kai KAMBRD ketina toliau tvarkyti asmens duomenis kitu tikslu nei tuo, kuriuo asmens duomenys buvo gauti, prieš tvarkydamas tuos duomenis, pateikia duomenų subjektui informaciją apie tą tikslą ir visą papildomą atitinkamą informaciją, kaip to reikalaujama Reglamento 13 straipsnio 3 dalyje ir 14 straipsnio 4 dalyje.

VI SKYRIUS DUOMENŲ SAUGOJIMAS IR SUNAIKINIMAS

34. Bendrųjų dokumentų saugojimo terminų rodyklėje, patvirtintoje Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymu Nr. V-100 „Dėl Bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo“, ir KAMBRD dokumentacijos plane nurodyti dokumentai, kuriuose yra asmens duomenų, saugomi Lietuvos vyriausiojo archyvaro nustatyta tvarka ir terminais pagal KAMBRD dokumentacijos planą. Kiti dokumentai, kuriuose yra asmens duomenų, ar duomenys, kurie saugomi ne dokumentuose (informacinėse sistemose, programose ir kt.), saugomi 2 mėnesius nuo dienos, kai pasiekiami tikslai, dėl kurių buvo tvarkomi asmens duomenys, išskyrus atvejus, kai ilgesnė duomenų saugojimo trukmė nustatyta įstatymuose ar kituose teisės aktuose arba vyksta teisminis procesas, susijęs su šiais asmens duomenimis, arba kitomis svarbiomis priežastimis objektyviai galima pagrįsti ilgesnį jų saugojimą.

KAMBRD asmens duomenys saugomi ne ilgiau, nei to reikia asmens duomenų tvarkymo tikslais. Kai asmens duomenys neberekalingi jų tvarkymo tikslais, jie sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduoti valstybės archyvams arba kurių saugojimo terminai nustatyti kituose teisės aktuose.

Suėjus asmens duomenų saugojimo terminams, teisės aktų nustatyta tvarka asmens duomenys sunaikinami taip, kad jų nebūtų galima atkurti ir atpažinti jų turinio.

VII SKYRIUS DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

35. Duomenų tvarkymo veiklos įrašai KAMBRD pildomi elektroniniu būdu. KAMBRD rekomenduojama naudoti KAM duomenų tvarkymo veiklos įrašų pildymo įrankį.

36. KAMBRD, kaip duomenų valdytojo, duomenų tvarkymo veiklos įrašuose nurodoma:

36.1. valdytojo (ar bendro duomenų valdytojo) pavadinimas ir kontaktiniai duomenys;

36.2. KAMBRD duomenų apsaugos pareigūno vardas, pavardė ir kontaktiniai duomenys (adresas, telefonas ir (ar) elektroninis paštas);

36.3. duomenų tvarkymo tikslai;

36.4. tvarkomų asmens duomenų kategorijos;

36.5. informacija apie duomenų tvarkymo (tvarkymo operacijos, kuriai reikalingi asmens duomenys) teisinį pagrindą;

36.6. duomenų subjektų kategorijos;

36.7. duomenų gavėjų, kuriems buvo arba bus atskleisti asmens duomenys, kategorijos, įskaitant duomenų gavėjus trečiojoje valstybėje ar tarptautines organizacijas;

36.8. asmens duomenų perdavimas trečiajai valstybei arba tarptautinei organizacijai (įskaitant tos trečiosios valstybės arba tarptautinės organizacijos pavadinimą) ir Reglamento 49 straipsnio 1 dalies antroje pastraipoje nurodytais duomenų perdavimo atvejais tinkamų apsaugos priemonių dokumentai;

36.9. jei įmanoma, numatomi įvairių kategorijų duomenų ištrynimo (saugojimo) terminai;

36.10. jei įmanoma, pateikiamas bendras techninių ir organizacinių saugumo priemonių aprašymas;

36.11. gali būti pateikiama ir kita reikalinga informacija;

36.12. jei asmens duomenys tvarkomi vadovaujantis Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais, įstatymu, duomenų tvarkymo veiklos įrašuose papildomai nurodoma informacija apie profiliavimą, jei jis atliekamas, ir asmens duomenų perdavimo trečiajai valstybei arba tarptautinei organizacijai, jei asmens duomenys perduodami, kategorijos.

37. KAMBRD pildomi ir KAMBRD, kaip duomenų tvarkytojo, duomenų veiklos įrašai.

38. KAMBRD padaliniai ar darbuotojai, atsakingi už asmens duomenų tvarkymą konkrečiais tikslais, pasikeitus asmens duomenų tvarkymui ar pastebėję netikslumą, nedelsdami informuoja KAMBRD duomenų apsaugos pareigūną pagal Taisyklių 36 punktą ir nurodo pasikeitusius ar

atnaujinamus duomenis. Įvertinęs gautą informaciją ir jei yra pagrindas, KAMBRD duomenų apsaugos pareigūnas atitinkamai atnaujina duomenų tvarkymo veiklos įrašus.

39. Pildant veiklos įrašus turi būti užtikrinamas įrašų pakeitimų atsekamumas – pakeitimai veiklos įrašuose atliekami fiksuojant pakeitimo datą ir pakeitimo turinį.

40. Valstybinės duomenų apsaugos inspekcijos prašymu duomenų tvarkymo veiklos įrašai pateikiami Valstybinei duomenų apsaugos inspekcijai, išskyrus atvejus, kai asmens duomenys tvarkomi nacionalinio saugumo ir gynybos tikslais.

VIII SKYRIUS

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI IR JŲ TYRIMAS

41. Asmens duomenų saugumo pažeidimai gali būti:

41.1. konfidencialumo pažeidimas – netyčinis (kai asmens duomenų saugumas pažeidžiamas neturint tikslo tai padaryti) arba neteisėtas asmens duomenų atskleidimas arba prieigos prie jų suteikimas asmenims, kurie neturi teisės susipažinti su asmens duomenimis;

41.2. vientisumo pažeidimas – netyčinis arba neteisėtas asmens duomenų pakeitimas;

41.3. prieinamumo pažeidimas – netyčinis arba neteisėtas prieigos prie asmens duomenų praradimas arba jų sunaikinimas.

42. Atsižvelgiant į aplinkybes, asmens duomenų saugumo pažeidimas gali būti ir bet kurių dviejų ar visų trijų Taisyklių 41.1–41.3 papunkčiuose nurodytų pažeidimų derinys.

43. KAMBRD darbuotojas, sužinojęs ar pats nustatęs galimą asmens duomenų saugumo pažeidimą arba gavęs informaciją apie galimą asmens duomenų saugumo pažeidimą iš visuomenės informavimo priemonių ar kitų šaltinių (toliau – asmens duomenų saugumo pažeidimo paaiškėjimas), privalo imtis šių veiksmų:

43.1. informuoti apie tai KAMBRD direktorių ir KAMBRD duomenų apsaugos pareigūną, pateikti jiems kuo tikslesnę turimą informaciją apie pažeidimą;

43.2. užpildyti Pranešimą apie galimą asmens duomenų saugumo pažeidimą (Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo 1 priedas) ir nedelsdamas, bet ne vėliau kaip per 2 darbo valandas nuo asmens duomenų saugumo pažeidimo paaiškėjimo KAMBRD darbuotojas privalo elektroniniu paštu arba per dokumentų valdymo sistemą perduoti jį KAMBRD darbuotojui, įgaliotam tirti asmens duomenų saugumo pažeidimus;

43.3. jei įmanoma, imtis priemonių galimam asmens duomenų saugumo pažeidimui pašalinti ir priemonių galimoms neigiamoms jo pasekmėms sumažinti arba pašalinti.

44. Jei galimas asmens duomenų saugumo pažeidimas yra susijęs su KAM valdomais asmens duomenimis, atliekami veiksmai, numatyti Asmens duomenų saugumo pažeidimų valdymo tvarkos apraše.

45. Jei galimas asmens duomenų saugumo pažeidimas yra susijęs su kitų duomenų valdytojų (ne KAMBRD ar KAM) valdomais, tačiau KAMBRD tvarkomais asmens duomenimis, atliekami veiksmai, numatyti KAMBRD su kitais duomenų valdytojais sudarytuose duomenų tvarkymo susitarimuose ir šiose Taisyklėse, Reglamente ar atitinkamai Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais (vykdomos duomenų tvarkytojui numatytos duomenų valdytojo informavimo ir kitos pareigos), įstatyme.

46. Darbuotojas, paskirtas tirti asmens duomenų saugumo pažeidimą, privalo:

46.1. nustatęs, kad asmens duomenų saugumo pažeidimas nepadarytas, nedelsdamas apie tai informuoti KAMBRD duomenų apsaugos pareigūną el. paštu brd.dap@kam.lt ir KAMBRD direktorių;

46.2. nustatęs, kad asmens duomenų saugumo pažeidimas yra padarytas, nedelsdamas, bet ne vėliau kaip per 24 valandas nuo pranešimo apie duomenų saugumo pažeidimą gavimo dienos jį iširti (išskyrus, kai yra objektyvios priežastys, dėl kurių negalima iširti nurodytu terminu) ir tyrimo rezultatus įforminti surašant į Taisyklių 52 punkte nurodytą ataskaitą.

47. Asmens duomenų saugumo pažeidimo tyrimo metu KAMBRD duomenų apsaugos pareigūnas, bendradarbiaudamas su darbuotoju, įgaliotam tirti asmens duomenų saugumo pažeidimą:

- 47.1. nustato, kokio tipo pažeidimas padarytas;
- 47.2. nustato asmens duomenų, kurių saugumas pažeistas, kategorijas, įskaitant specialių kategorijų asmens duomenis;
- 47.3. nustato asmens duomenų pažeidimo priežastis, lėmusias asmens duomenų saugumo pažeidimą;
- 47.4. nustato asmens duomenų pažeidimo apimtį (duomenų subjektų, su kurių asmens duomenimis susijęs pažeidimas, kategorijos ir jų skaičius);
- 47.5. nustato ir įvertina esamas ir (ar) galimas pasekmes ir žalą, padarytą duomenų subjektui (subjektams);
- 47.6. įvertina galimą pavojų duomenų subjektų teisėms ir laisvėms;
- 47.7. pasitelkia kitų KAMBRD darbuotojų pagalbą, jei yra būtina;
- 47.8. nustato, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas (pvz., naudoti atsargines kopijas, siekiant atkurti prarastus ar sugadintus duomenis ar kt.);
- 47.9. įvertina, ar būtina nedelsiant pranešti duomenų subjektui ir Valstybinei duomenų apsaugos inspekcijai apie asmens duomenų saugumo pažeidimą.
48. Pavojus duomenų subjekto teisėms ir laisvėms vertinamas objektyviai, įvertinus konkrečias pažeidimo aplinkybes, įskaitant pavojaus tikimybę ir rimtumą, ir atsižvelgiant į:
- 48.1. asmens duomenų saugumo pažeidimo tipą (Taisyklių 41.1–41.3 papunkčiai);
- 48.2. asmens duomenų kategorijas (pvz., specialių kategorijų asmens duomenys), pobūdį, asmens duomenų, kurių saugumas pažeistas, kiekį;
- 48.3. galimybę lengvai nustatyti asmens tapatybę, pasinaudojant asmens duomenimis, kurie yra pažeidimo objektas;
- 48.4. pasekmių rimtumą duomenų subjektui;
- 48.5. su duomenų subjektu susijusius ypatumus;
- 48.6. asmenų, kuriems pažeidimas daro poveikį, skaičių.
49. Vertinant pavojų duomenų subjekto teisėms ir laisvėms laikoma, kad asmens duomenų saugumo pažeidimas, galintis kelti pavojų duomenų subjektų teisėms ir laisvėms, yra toks, dėl kurio laiku nesuimtus tinkamų priemonių kyla grėsmė duomenų subjektų sveikatai ir (ar) gyvybei, grėsmė patirti materialinę ar nematerialinę žalą, pvz., prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinais panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala. Preziumuojama, kad pažeidimas kelia pavojų duomenų subjekto teisėms ir laisvėms, kai pažeidimas yra susijęs su specialių kategorijų asmens duomenimis.
50. Įvertinus pavojų duomenų subjekto teisėms ir laisvėms nustatoma, kad:
- 50.1. pavojaus duomenų subjekto teisėms ir laisvėms nėra (žema rizikos tikimybė): asmuo gali susidurti su nepatogumais (sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);
- 50.2. dėl asmens duomenų saugumo pažeidimo yra arba gali kilti nedidelis pavojus duomenų subjektų teisėms ir laisvėms (vidutinė rizikos tikimybė): asmuo gali patirti didelių nepatogumų, kuriuos jis galės įveikti nepaisydamas tam tikrų sunkumų (papildomos išlaidos, priegos prie reikalingų resursų praradimas, nedideli fiziniai negalavimai ir pan.);
- 50.3. dėl asmens duomenų saugumo pažeidimo yra arba gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms (didelė rizikos tikimybė): asmuo gali patirti dideles pasekmes ir norint jas ištaisyti / pašalinti reikės susidurti su rimtais sunkumais (lėšų praradimas, finansinių institucijų įtraukimas į juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.). Labai didelis pavojus fizinių asmenų teisėms ir laisvėms, kai asmuo gali turėti labai dideles ar net negrįžtamas pasekmes, kurių negalės ištaisyti / pašalinti (pvz., negalėjimas dirbti, ilgalaikiai negalavimai, mirtis ir pan.).
51. Kai dėl asmens duomenų saugumo pažeidimo kyla arba gali kilti pavojus fizinių asmenų teisėms ir laisvėms, nedelsiant ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai

KAMBRD sužino apie asmens duomenų saugumo pažeidimą, apie tai pranešama Valstybinei duomenų apsaugos inspekcijai užpildant Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. 1T-82 (1.12.E) „Dėl Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“ patvirtintą formą. Už formos pildymą atsakingas KAMBRD duomenų apsaugos pareigūnas, jis konsultuojasi su asmeniu, paskirtu tirti asmens duomenų saugumo pažeidimą.

52. Darbuotojas, kuriam paskirta atlikti tyrimą, šių Taisyklių nustatyta tvarka atlikęs asmens duomenų saugumo pažeidimo tyrimą, bendradarbiaudamas su KAMBRD duomenų apsaugos pareigūnu, nedelsdamas surašo Asmens duomenų saugumo pažeidimo ataskaitą, ją pasirašo ir pateikia registruoti (pildoma Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo 2 priede nustatyta forma).

53. Pasirašyta ir užregistruota darbuotojo, įgalioto tirti asmens duomenų saugumo pažeidimus, Asmens duomenų saugumo pažeidimo ataskaita per dokumentų valdymo sistemą DokVIS pateikiama tvirtinti KAMBRD direktoriui.

54. Prireikus KAMBRD direktorius, atsižvelgdamas į Asmens duomenų saugumo pažeidimo ataskaitą, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl asmens duomenų saugumo pažeidimo, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus. Už priemonių plano rengimą atsakingi KAMBRD duomenų apsaugos pareigūnas ir darbuotojas, įgaliotas tirti asmens duomenų saugumo pažeidimą.

55. Kai įtariama, kad asmens duomenų saugumo pažeidimas turi nusikalstamos veikos požymių, KAMBRD darbuotojas, įgaliotas tirti asmens duomenų saugumo pažeidimus, inicijuoja informacijos apie galimai padarytą nusikalstamą veiką pateikimą atitinkamoms valstybės institucijoms, įgaliotoms atlikti ikiteisminį tyrimą.

56. Kai dėl asmens duomenų saugumo pažeidimo kyla arba gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, KAMBRD duomenų apsaugos pareigūnas kartu su darbuotoju, įgaliotu tirti asmens duomenų saugumo pažeidimą, nedelsdami ir, jeigu galima, praėjus ne daugiau kaip 72 valandoms nuo asmens duomenų saugumo pažeidimo paaiškėjimo, apie tai praneša duomenų subjektui.

57. Pranešime duomenų subjektui aiškia ir paprasta kalba turėtų būti pateikiama ši informacija:

57.1. asmens duomenų saugumo pažeidimo pobūdžio aprašymas;

57.2. duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys (telefonas, adresas ir (arba) el. paštas);

57.3. tikėtinų asmens duomenų saugumo pažeidimo pasekmių aprašymas;

57.4. priemonių, kurių ėmėsi arba pasiūlė imtis, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant (kai tinkama) priemonės galimoms neigiamoms jo pasekmėms sumažinti, aprašymas (pvz., kad apie pažeidimą yra informuota Valstybinė duomenų apsaugos inspekcija ir kad gautas patarimas dėl pažeidimo tvarkymo ir jo poveikio sumažinimo; siūlymas duomenų subjektui pasikeisti slaptažodžius ir kt.);

57.5. kita svarbi informacija, susijusi su asmens duomenų saugumo pažeidimu.

Duomenų subjektai apie asmens duomenų saugumo pažeidimą turi būti informuoti tiesiogiai, pvz., siunčiant jiems pranešimą elektroniniu paštu ar kitu efektyviu būdu, kad būtų maksimaliai užtikrinta galimybė tinkamai pranešti informaciją visiems nukentėjusiems asmenims. Jei duomenų subjektui reikia pranešti atskiru raštu, KAMBRD duomenų apsaugos pareigūnas parengia rašto projektą ir suderinęs jį su darbuotoju, paskirtu tirti asmens duomenų saugumo pažeidimą, teikia pasirašyti KAMBRD direktoriui.

58. Visi asmens duomenų saugumo pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta Valstybinei duomenų apsaugos inspekcijai, turi būti fiksuojami (įrašomi) Asmens duomenų saugumo pažeidimų apskaitos žurnale (pildoma Asmens duomenų saugumo pažeidimų aprašo 3 priede numatyta forma). Už asmens duomenų saugumo pažeidimų žurnalo pildymą atsakingas KAMBRD duomenų apsaugos pareigūnas.

59. Asmens duomenų saugumo pažeidimų apskaitos žurnale nurodoma:

59.1. visi su asmens duomenų saugumo pažeidimu susiję faktai: pažeidimo priežastys, kas įvyko ir kokie asmens duomenys pažeisti;

59.2. asmens duomenų saugumo pažeidimo pasekmės ir pavojus fizinių asmenų teisėms ir laisvėms;

59.3. taisomieji veiksmai, kurių buvo imtasi;

59.4. su asmens duomenų saugumo pažeidimu susijusių sprendimų priėmimo motyvai (pvz., kodėl nuspręsta nepranešti apie pažeidimą Valstybinei duomenų apsaugos inspekcijai ir (arba) duomenų subjektui, t. y. kodėl nuspręsta, jog pažeidimas neturėtų sukelti pavojaus fizinių asmenų teisėms ir laisvėms ir kt.);

59.5. pranešimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys, jeigu pranešimą vėluojama pateikti ar pranešimas teikiamas etapais (tuo atveju, jei reikia pranešti);

59.6. informacija, susijusi su pranešimu duomenų subjektui (pvz., ar buvo pranešta, kodėl nepranešta);

59.7. kita svarbi informacija, susijusi su asmens duomenų saugumo pažeidimu (pvz., tyrimo metu nustatyta, jog faktiškai pažeidimo nebuvo, tik saugumo incidentas).

60. Asmens duomenų saugumo pažeidimų apskaitos žurnalas tvarkomas elektronine forma ir saugomas Lietuvos vyriausiojo archyvaro nustatyta tvarka KAMBRD dokumentacijos plane nurodytais terminais.

IX SKYRIUS

POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

61. Tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, naudojant naujas technologijas ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, žmogaus teisėms ir laisvėms gali kilti didelis pavojus, KAMBRD, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą. Nustatant, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų žmogaus teisėms ir laisvėms, atsižvelgiama į 29 straipsnio duomenų apsaugos darbo grupės 2017 m. balandžio 4 d. „Poveikio duomenų apsaugai vertinimo (PDAV) gaires, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų“ (toliau – 29 darbo grupės PDAV gairės). Panašius didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą.

62. Už poveikio duomenų apsaugai vertinimo atlikimą yra atsakingi KAMBRD padaliniai, kurie numato asmens duomenų tvarkymą / tvarko asmens duomenis, kai dėl šių duomenų tvarkymo operacijų reikia atlikti poveikio duomenų apsaugai vertinimą. Atliekant vertinimą konsultuojamasi su KAMBRD duomenų apsaugos pareigūnu. Poveikio duomenų apsaugai procesas dokumentuojamas, užpildant KAS asmens duomenų tvarkymo taisyklių 9 priede pateiktą Poveikio duomenų apsaugai vertinimo krašto apsaugos sistemoje ataskaitos formą. Užpildyta forma registruojama dokumentų valdymo sistemoje DokVIS.

63. Atliekant poveikio duomenų apsaugai vertinimą, vadovaujamosi Asmens duomenų, tvarkomų teisėsaugos ar nacionalinio saugumo tikslais, įstatymo 25 straipsniu arba Reglamento 35 straipsniu ir Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašų, patvirtintu Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T-35 (1.12.E) „Dėl Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašo patvirtinimo“, atsižvelgiama į 29 darbo grupės PDAV gaires.

64. Poveikio duomenų apsaugai vertinimas atliekamas vadovaujantis Direktyvos 95/46/EB 29 straipsnio duomenų apsaugos darbo grupės 2017 m. balandžio 4 d. priimtų Poveikio duomenų apsaugai vertinimo gairių 2 priede („Priimtino PDAV kriterijai“) nurodytais poveikio duomenų apsaugai vertinimo kriterijais ir laikantis pritaikytosios ir standartizuotosios duomenų apsaugos principų.

65. Poveikio duomenų apsaugai vertinimas atliekamas pagal šiuos kriterijus:

65.1. numatytų duomenų tvarkymo operacijų aprašymas (apreptis, duomenų tvarkymo tikslai, įskaitant, kai taikoma, KAMBRD teisėtus interesus, renkami asmens duomenys, duomenų gavėjų tapatybė, saugojimo laikotarpis);

65.2. duomenų tvarkymo operacijų reikalingumo ir proporcingumo, palyginti su tikslais, vertinimas;

65.3. duomenų subjektų teisėms ir laisvėms kylančių pavojų vertinimas;

65.4. pavojams pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi Reglamento, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus.

66. Atlikęs poveikio asmens duomenų apsaugai vertinimą ir nustatęs, kad tvarkant duomenis gali kilti didelis pavojus, kai asmens duomenys tvarkomi vadovaujantis Reglamentu, KAMBRD vykdo išankstines konsultacijas su Valstybine duomenų apsaugos inspekcija. Išankstinės konsultacijos vykdomos vadovaujantis Reglamento 36 straipsniu.

67. Prireikus KAMBRD duomenų apsaugos pareigūnas stebi poveikio duomenų apsaugai vertinimą ir pataria, konsultuoja dėl jo atlikimo.

68. Poveikio asmens duomenų apsaugai vertinimas gali būti atliekamas dėl KAMBRD tvarkomų kitų asmens duomenų valdytojų valdomų asmens duomenų, jei tai nustatyta KAMBRD ir kito duomenų valdytojo asmens duomenų tvarkymo susitarime arba teisės akte.

X SKYRIUS BAIGIAMOSIOS NUOSTATOS

69. Jeigu KAMBRD tvarkoma informacija turi būti skelbiama viešai ir joje yra viešai neskelbtinų duomenų (valstybės, tarnybos, profesinių, komercinių ar kitų teisės aktų saugomų paslapčių arba kitokių neskelbtinų duomenų) ar asmens duomenų (fizinių asmenų asmens kodai, gyvenamųjų vietų adresai, gimimo datos ir vietos, valstybiniai automobilių numeriai, sveikatos duomenys ir kita), parengiama viešai skelbtina teksto versija, kurioje asmens duomenys pakeičiami taip, kad duomenų subjekto tapatybės nebūtų galima nustatyti. Nuasmeninant informaciją rekomenduotina vadovautis Valstybinės duomenų apsaugos inspekcijos 2020 m. rugpjūčio 5 d. rekomendacija „Nuasmeninimo metodai“.

70. KAMBRD rengiamų Lietuvos Respublikos teisės aktų, reglamentuojančių asmens duomenų tvarkymą, projektuose nurodomi duomenų tvarkymo tikslai, tvarkytini asmens duomenys ir kiti duomenų tvarkymo reikalavimai, kuriais siekiama užtikrinti teisėtą asmens duomenų tvarkymą.

71. KAMBRD duomenų apsaugos pareigūnas atsakingas, kad šios Taisyklės būtų periodiškai, bet ne rečiau kaip 1 kartą per metus peržiūrimos ir, esant poreikiui, atnaujinamos, taip pat vykdo Taisyklių įgyvendinimo stebėseną ir kontrolę, kaip laikomasi šiose Taisyklėse įtvirtintų reikalavimų.

72. KAMBRD direktorius turi teisę įgalioti KAMBRD darbuotojus tvarkyti tam tikros kategorijos asmens duomenis.

73. KAMBRD darbuotojas, netinkamai vykdamas Taisyklių, Reglamento, kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą, reikalavimus, atsako įstatymų nustatyta tvarka.

74. Visi darbuotojai pasirašytinai arba dokumentų valdymo sistemoje DokVIS supažindinami su šiomis Taisyklėmis, o naujai į KAMBRD priimti darbuotojai ir duomenų tvarkytojai su šiomis Taisyklėmis supažindinami KAMBRD duomenų apsaugos pareigūno ar kito KAMBRD vadovo paskirto atsakingo asmens, iki jiems pradėdant atlikti bet kokius veiksmus su KAMBRD valdomais asmens duomenimis.