

**VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA****SPRENDIMAS**

2026 m. spalio 15 d. Nr. 3R-1815 (2.13-1.E)

Vilnius

Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) 2026-04-03 gavo Migracijos departamento prie Lietuvos Respublikos Vidaus reikalų ministerijos (toliau – Migracijos departamentas) pirminį pranešimą apie asmens duomenų saugumo pažeidimą (toliau – ADSP) (Inspekcijos reg. Nr. 1R-2584 (2.23 Mr)) bei 2026-04-27 gavo patikslintą pranešimą apie ADSP (Inspekcijos reg. Nr. 1R-3308 (2.23 Mr)) ir Valstybinės duomenų apsaugos inspekcijos direktoriaus 2026 m. gegužės 15 d. įsakymu Nr. 1T-65 (1.12.E) nusprendė savo iniciatyva pradėti tyrimą, susijusį su galimu 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 – BDAR) nuostatų pažeidimu, Migracijos departamento atžvilgiu.

Inspekcija 2026-04-13 gavo VĮ Registrų centro (toliau – Registrų centras) raštą dėl informacijos pateikimo (Inspekcijos reg. Nr. 1R-2759 (2.23 Mr)) bei 2026-05-07 gavo pranešimą apie ADSP (Inspekcijos reg. Nr. 1R-3638 (2.23 Mr)) ir Valstybinės duomenų apsaugos inspekcijos direktoriaus 2026 m. gegužės 15 d. įsakymu Nr. 1T-66 (1.12.E) nusprendė savo iniciatyva pradėti tyrimą, susijusį su galimu BDAR nuostatų pažeidimu, Registrų centro atžvilgiu.

Inspekcija 2026-06-26 gavo Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) raštu Nr. 6K-766 (4.2 Mr) (Inspekcijos reg. Nr. 1R-5358 (2.23 Mr)) pateiktą Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) Kibernetinio incidento tyrimo ataskaitą, kurioje nurodytos aplinkybės, susijusios su neteisėta prieiga prie dviejų Migracijos departamento darbuotojų el. pašto paskyrų, ir Valstybinės duomenų apsaugos inspekcijos direktoriaus 2026 m. liepos 23 d. įsakymu Nr. 1T-90 (1.12.E) nusprendė savo iniciatyva pradėti tyrimą, susijusį su galimu BDAR nuostatų pažeidimu, Informatikos ir ryšių departamento atžvilgiu.

Inspekcija, atlikusi Informatikos ir ryšių departamento, Migracijos departamento ir Registrų centro tyrimus (toliau kartu – tyrimas),

n u s t a t ė:**Inspekcijai pateikta informacija**

Migracijos departamentas 2026-04-03 pateikė pirminį pranešimą apie ADSP (Inspekcijos reg. Nr. 1R-2584 (2.23 Mr)), kuriame nurodė, jog Migracijos departamento duomenų apsaugos pareigūnė 2026-04-03 buvo informuota apie tai, kad iš dviejų darbuotojų paskyrų, neturint teisėto pagrindo, buvo jungiamasi prie Nekilnojamojo turto registro (toliau – NTR). Taip pat nurodė, jog yra atliekamas tyrimas, o darbuotojų paskyros, iš kurių buvo jungiamasi prie NTR, užblokuotos, bei pažymėjo, kad informacija apie atlikto tyrimo rezultatus bus pateikta papildomai.

Registrų centras 2026-04-13 pateikė raštą dėl informacijos pateikimo (Inspekcijos reg. Nr. 1R-2759 (2.23 Mr)), kuriame nurodė, jog iš Migracijos departamento buvo gauta informacija apie galimai prarastus prisijungimo prie NTR duomenis ir galimą jų panaudojimą jungiantis prie NTR ir gaunant NTR duomenis. Pažymėjo, kad detalesnė informacija pateikta nebuvo, tačiau, reaguojant į situaciją, buvo užblokuotos įtarimus keliančios Migracijos departamento darbuotojų paskyros, IP adresai, inicijuotas priverstinis slaptažodžių keitimas, nustatyta galimybė atlikti reikiamus veiksmus tik iš konkrečių Migracijos departamentui priskirtų IP adresų. Taip pat nurodė, kad yra atliekami tyrimai ir patikrinimai, juos baigus ir nustačius visas aplinkybes apie tai bus pranešta papildomai.

Registrų centras 2026-05-07 pateikė pranešimą apie ADSP (Inspekcijos reg. Nr. 1R-3638 (2.23 Mr)), kuriame nurodė, kad 2026-04-01 gavęs Migracijos departamento prašymą atlikti išsamų patikrinimą dėl Migracijos departamento darbuotojo išorinės naudotojų naršyklės¹ prisijungimo duomenų ir NTR duomenų gavimo bei atlikęs Migracijos departamento darbuotojos veiksmų analizę pastebėjo didelius duomenų paieškos ir gavimo iš NTR kiekius, taip pat nedidelės apimties paieškas Juridinių asmenų registre (toliau – JAR) ir JAR išrašų peržiūras nuo 2026-01-06. Taip pat nurodė, kad Registrų centras atliko kitų Migracijos departamento naudotojų, turinčių prieigos teises prie išorinės naudotojų naršyklės pagal duomenų teikimo sutartis, veiksmų analizę ir nustatė kito naudotojo didelį duomenų paieškų ir duomenų gavimo kiekį tuo pačiu laikotarpiu. Registrų centras nurodė, kad ADSP metu atskleisti 678 976 NTR išrašai (538 226 duomenų subjektai) ir 33 juridinių asmenų JAR išrašai (66 duomenų subjektai). Taip pat pažymėjo, jog Registrų centras nėra gavęs oficialiai patvirtintos informacijos apie tai, ar duomenų gavėjo (Migracijos departamento) pusėje yra įvykęs ADSP ir kokios galėtų būti to priežastys. Nepaisant to, įtariant galimus piktavališkus veiksmus NTR (didelis užklausų kiekis; užklausų teikimas ne darbo valandomis; aplinkybė, jog duomenų gavėjas nepatvirtino, kad įtarimus keliančios užklausos teiktos teisėtai), taip pat įtarimus keliančių naudotojų atliktas paieškas ir peržiūras JAR, 2026-05-07 nuspręsta atvejį laikyti ADSP.

Atsižvelgiant į pateiktą informaciją, Inspekcija 2026-04-16, 2026-05-21, 2026-06-29 raštais (Inspekcijos reg. Nr. atitinkamai 2R-2166 (2.23 Mr), 2R-2876 (2.23 Mr) ir 2R-3923 (2.14 E)) kreipėsi į Migracijos departamentą dėl informacijos pateikimo. Inspekcijoje 2026-04-27, 2026-05-28 ir 2026-07-10 gauti Migracijos departamento atsakymai (Inspekcijos reg. Nr. atitinkamai 1R-3308 (2.23 Mr), 1R-4344 (2.23 Mr) ir Nr. 1R-5766 (2.14 E)) (toliau kartu – Migracijos departamento atsakymas).

Taip pat Inspekcija, atsižvelgdama į pateiktą informaciją, 2026-05-20 ir 2026-06-30 raštais (Inspekcijos reg. Nr. atitinkamai 2R-2845 (2.23 Mr) ir 2R-3961 (2.14 E)) kreipėsi į Registrų centrą dėl informacijos pateikimo. Inspekcijoje 2026-05-28 ir 2026-07-10 gauti Registrų centro atsakymai (Inspekcijos reg. Nr. atitinkamai 1R-4302 (2.23 Mr) ir 1R-5769 (2.14 E)) (toliau kartu – Registrų centro atsakymas).

Migracijos departamentas atsakyme nurodė, kad 2026-03-27 ir 2026-04-01 gavo Informatikos ir ryšių departamento paklausimus dėl informacijos pateikimo, kuriuose nurodyta, jog Migracijos departamento darbuotoja (naudotojas [DUOMENYS NESKELBTINI]) 2026-02-02 ir 2026-02-12 tikrino duomenis apie [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI] priklausantį nekilnojamąjį turtą. Buvo pradėtas tyrimas bei aplinkybių patikslinimas. Migracijos departamento darbuotoja nurodė, kad šių duomenų NTR netikrino, o naudotojo vardu [DUOMENYS NESKELBTINI] nesinaudojo nuo 2024 metų. Darbuotojos teigimu, prisijungimo duomenų niekam neperdavė. Pažymėjo, jog iš minėtų paklausimų matyti, kad duomenų tikrinimai NTR buvo atlikti iš to paties IP adreso [DUOMENYS NESKELBTINI] (nepriklausančio Migracijos departamentui), nustatyta, kad šis IP adresas galimai veikia Malaizijoje. Atsižvelgdamas į tai, Migracijos departamentas 2026-04-01 raštu Registrų centro bei Informatikos ir ryšių departamento paprašė atlikti išsamų patikrinimą dėl galimo Migracijos departamento darbuotojos prisijungimo duomenų

¹ Registrų centro tvarkomų duomenų teikimo būdas duomenų teikimo sutartyse nurodytiems naudotojams.

pasisavinimo ir neteisėto duomenų gavimo iš NTR. Registrų centro iniciatyva 2026-04-02 buvo surengtas nuotolinis pokalbis, kurio metu paaiškėjo, kad galėjo būti užvaldyta dar vienam Migracijos departamento darbuotojui Registrų centro suteikta paskyra. Registrų centras 2026-04-08 informavo, kad atlikęs naudotojo [DUOMENYS NESKELBTINI] veiksmų analizę pastebėjo didelius duomenų paieškos ir gavimo iš registro kiekius nuo 2026-01-06, taip pat, atlikus kitų Migracijos departamento naudotojų veiksmų registre analizę, nustatė didelius naudotojo [DUOMENYS NESKELBTINI] duomenų paieškų ir gavimo iš registro kiekius tuo pačiu laikotarpiu. Pagal registro žurnalinių įrašų duomenis, per nurodytą laikotarpį užfiksuotas itin didelis duomenų paieškos ir gavimo mastas: atlikta apie 936 tūkst. veiksmų, iš kurių daugiausia sudarė registro įrašų formavimas (apie 679 tūkst.), daiktų paieška pagal adresą (apie 240 tūkst.) ir adresų paieška (apie 17 tūkst.). Didžioji dalis veiksmų atlikta naudotoju [DUOMENYS NESKELBTINI] (atitinkamai apie 472 tūkst., 196 tūkst. ir 14,8 tūkst.), likusi dalis – naudotoju [DUOMENYS NESKELBTINI] (apie 207 tūkst., 43,5 tūkst. ir 2,2 tūkst.). [DUOMENYS NESKELBTINI]². Registrų centrui atlikus analizę nustatyta, kad laikotarpiu nuo 2026-01-01 iki 2026-04-30 nefiksuota naudotojos [DUOMENYS NESKELBTINI] prisijungimo prie NTR ir JAR fakto ar kitų veiksmų.

Migracijos departamentas atsakyme pažymėjo, kad Registrų centras duomenis teikia vadovaujantis NTR 2013 sutartimi³ ir JAR 2017 sutartimi⁴. Pagal minėtas sutartis ir jų priedus Registrų centras galėjo leisti Migracijos departamentui naudotis duomenų teikimo sistema tik iš dviejų išorinių IP adresų ([DUOMENYS NESKELBTINI]), tačiau tyrimo metu nustatyta, kad Registrų centras duomenis teikė ir kitais IP adresais, esančiais Lietuvoje, Bulgarijoje, Nyderlanduose ir Malaizijoje. Pažymi, kad Migracijos departamentas, įtaręs, jog prisijungimo slaptažodžiai tapo žinomi kitiems asmenims, nedelsiant, 2026-04-01, apie tai informavo VĮ Registrų centrą.

Migracijos departamentas atsakyme atkreipė dėmesį, kad darbuotojų prieigos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Vidaus reikalų ministerija) valdomų informacinių sistemų, registrų ir kitų IT išteklių yra suteikiamos centralizuotai, nutraukus darbo santykius su darbuotoju, jo paskyros (prieiga prie IT išteklių, el. pašto ir kompiuterizuotos darbo vietos) yra panaikinamos automatiškai būdu. Prieigos prie išorės sistemų, kurios nėra Vidaus reikalų ministerijos valdomoje infrastruktūroje, tvarkomos atskirai pagal sudarytas duomenų gavimo sutartis. Migracijos departamento darbuotojai, vykdančys tiesiogines darbo funkcijas, suteiktomis prieigomis prie išorinių sistemų ar registrų naudojasi pagal poreikį (t. y. darbuotojas kurį laiką gali nesinaudoti suteiktomis prieigomis, tačiau jos būtinos darbo funkcijų vykdymui).

Registrų centras atsakyme nurodė, jog atlikus kibernetinio incidento analizę nustatyta, kad incidentą sukėlė trečiosios šalys, pasinaudojusios užvaldytais Migracijos departamento paskyrų duomenimis ([DUOMENYS NESKELBTINI], [DUOMENYS NESKELBTINI] ir [DUOMENYS NESKELBTINI]). Su nagrinėjamu ADSP susijusiu atveju aktualus duomenų teikimo būdas, kai duomenų teikimo sutartis su Registrų centru sudariusių duomenų gavėjų naudotojai jungiasi prie Registrų centro savitarnos portalo „Turintiems sutartį“. Iki šiol tokie naudotojai jungėsi su identifikaciniais duomenimis (naudotojo vardas ir slaptažodis), o kelių faktorių autentifikavimas (MFA) nebuvo taikomas. Jungiantis prie NTR ir JAR duomenų gavėjams pagal duomenų gavimo sutartis taikomas IP filtravimas, tačiau ne visais atvejais. Nagrinėjamo incidento atveju naudotojams, kurių prisijungimo duomenys buvo paveikti, IP filtravimas nebuvo taikomas. Paaiškino, jog NTR 2013 sutarties ir JAR 2017 sutarties pagrindu Migracijos departamentas teikė 2021-02-01 ir 2023-07-12 prašymus į duomenų naudotojų sąrašus įtraukti juose nurodytus darbuotojus. Šiuose prašymuose nebuvo

² Atlikus naudotojų veiksmų analizę nustatytas neįprastai didelis duomenų paieškos ir gavimo iš registrų mastas, taip pat nustatyti prisijungimai iš Migracijos departamentui nepriskirtų IP adresų.

³ Registrų centro ir Vidaus reikalų ministerijos Nekilnojamojo turto registro duomenų teikimo 2013-04-04 sutartis Nr. NTRI-3941 (toliau – NTR 2013 sutartis).

⁴ Registrų centro ir Migracijos departamento 2017-11-24 duomenų teikimo sutartis Nr. RD-1 (su visais papildomais susitarimais) (toliau – JAR 2017 sutartis).

nurodyti statiniai (fiksiuoti) viešieji IP adresai, iš kurių jungsis prašymuose nurodyti darbuotojai, taip Migracijos departamentui išreiškiant pageidavimą šiems naujiems naudotojams duomenų teikimo sistema leisti naudotis kreipiantis iš bet kurio IP adreso ir laikant tokį savo veiksmą dėl prieigų suteikimo tinkamu. Paaiškino, kad saugos įrangoje nėra kaupiami tipiniai naudotojų veiksmų aplikacijose (pvz., savitarnoje) žurnaliniai įrašai, tokie kaip duomenų peržiūros, skaitymo ar atsisiuntimo faktai, o iki incidento atliekamų užklausų kiekiai buvo stebimi ir analizuojami duomenų gavėjo, bet ne konkretaus jo naudotojo, lygmeniu (šiuo atveju duomenų gavėjas pagal NTR 2013 sutartį buvo Vidaus reikalų ministerija, kurio užklausų kiekis dėl duomenų gavimo iš registų ir informacinių sistemų kitų duomenų gavėjų bendrame užklausų kontekste nebuvo neįprastai didelis). Dėl perspėjimų apie jungimąsi iš užsienio šalių IP adresų paaiškino, kad paveiktoms naudotojų paskyroms nebuvo iš anksto deklaruoti ir Registų centrui patvirtinti statiniai (fiksiuoti) viešieji IP adresai, dėl šios priežasties automatiniai perspėjimai (angl. *alerts*) nebuvo fiksuojami, nes tokie jungimaisi buvo galimi pagal Migracijos departamento teiktus prašymus dėl įtraukimo į naudotojų sąrašus. Pažymi, kad jeigu naudotojų paskyroms, duomenų gavėjo nurodymu, būtų taikomas statinis (fiksuotas) viešasis IP adresas, prieigos bandymai būtų atmesti. Pažymi ir tai, kad pagal duomenų teikimo sutartis sutarties šalys (duomenų gavėjai) privalo nedelsdamos informuoti Registų centrą apie pasikeitimus, susijusius su jų naudotojais (darbo santykių pabaigą, kontaktinių duomenų pasikeitimus, poreikio turėti prieigas nebuvimą (pvz., pasikeitus darbo funkcijoms, kai turėtos prieigos tampa neberekalingomis naujų darbo funkcijų atlikimui)). Atitinkamai nenaudojamų naudotojų paskyrų peržiūra buvo vykdoma gavus duomenų gavėjų pranešimus. Šiuo konkrečiu atveju iki incidento Migracijos departamentas nebuvo pateikęs jokio pranešimo Registų centrui apie tai, kad kuriam nors iš incidento paveiktų naudotojų poreikis dėl prieigų prie informacinių sistemų išnyko.

Registų centras atsakyme dėl duomenų subjektų informavimo paaiškino, kad 2026-05-07 buvo kreiptasi į Lietuvos Respublikos generalinę prokuratūrą (toliau – Generalinė prokuratūra) prašant pateikti informaciją apie sprendimą dėl ikiteisminio tyrimo medžiagoje esančių incidento duomenų viešinimo BDAR nustatyta tvarka ir 2026-05-14 gautas atsakymas, jog BDAR 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija ir priemonės neturi ikiteisminio tyrimo duomenų požymių. Pažymėjo, jog paraleliai vyko aktyvus pasirengimas atvejui, jeigu duomenų subjektų informavimas apie ADSP bus suderinamas su ikiteisminio tyrimo vykdymu, t. y. rengiamas specialus techninis sprendimas Registų centro savitarnos sistemoje, kuriuo naudodamiesi asmenys, tinkamai save identifikavę, galėtų patys patikrinti, ar jų asmens duomenys, esantys NTR, buvo atskleisti, taip pat gauti BDAR 34 straipsnyje numatytą informaciją. Nuo 2026-05-25, baigus techninio sprendimo įgyvendinimo darbus, šis sprendimas tapo pasiekiamas visiems duomenų subjektams, kurie jungiasi prie Registų centro savitarnos. Taip pat informacija, ar konkretaus asmens duomenys, esantys NTR, buvo atskleisti, teikiama visuose Registų centro klientų aptarnavimo padaliniuose. Be to, duomenų subjektams apie ADSP pranešta ir viešais pranešimais Registų centro svetainėje, Facebook paskyroje, naujienų portaluose. Papildomai nurodė, kad specialus techninis sprendimas Registų centro savitarnos sistemoje neapima duomenų subjektų, kurių asmens duomenys buvo atskleisti suformavus JAR išrašus, ir atsižvelgiant į tai, kad buvo nutekinti 30 juridinių asmenų išplėstiniai išrašai ir 3 juridinių asmenų išplėstiniai išrašai su istorija, o nutekintuose išrašuose yra nurodytas kontaktinis duomenų subjektų adresas, šie asmenys informuojami individualiai, pranešimus apie ADSP išsiunčiant paštu.

Inspekcija, atsižvelgdama į tai, kad apie įvykusį kibernetinį incidentą buvo informuotas ir NKSC, 2026-06-17 raštu Nr. 2R-3638 (2.23 Mr) kreipėsi į NKSC dėl informacijos pateikimo. Inspekcijoje 2026-06-26 gautas NKSC atsakymas (Inspekcijos reg. Nr. 1R-5358 (2.23 Mr)). NKSC kartu su atsakymu pateikė Informatikos ir ryšių departamento Saugumo operacijų skyriaus 2026-05-27 kibernetinio incidento tyrimo ataskaitą (toliau – Ataskaita).

Ataskaitoje nurodyta, kad [DUOMENYS NESKELBTINI]⁵.

Atsižvelgiant į pateiktą informaciją, Inspekcija 2026-07-24 raštu Nr. 2R-4454 (2.23 Mr) kreipėsi į Informatikos ir ryšių departamentą dėl informacijos pateikimo. Inspekcijoje 2026-08-07 gautas atsakymas (Inspekcijos reg. Nr. 1R-6517 (2.23 Mr)) (toliau – Informatikos ir ryšių departamento atsakymas).

Informatikos ir ryšių departamentas atsakyme nurodė, kad [DUOMENYS NESKELBTINI]⁶. Be to, patvirtino, kad ADSP metu buvo naudojama Microsoft Exchange Server 2019 sistema, kuri nepalaikė galimybės naudoti kelių faktorių autentifikavimą. Prisijungimai prie el. pašto iš užsienio nebuvo laikomi savaiminiu faktoriumi, rodančiu neteisėtą veiklą, nes el. pašto naudotojai turėjo poreikį prieiti prie jo ir būdami užsienyje (išvykus į komandiruotę, nuotolinio darbo metu ir pan.).

Lietuvos Respublikos teisingumo ministerija (toliau – Teisingumo ministerija) 2026-07-13 rašte (Inspekcijos reg. Nr. 1R-5809 (2.14 E)) Inspekcijai nurodė, kad Registrų centras, kaip duomenų tvarkytojas, asmens duomenis tvarko vadovaudamasis BDAR 28 straipsnio 3 dalimi. Pažymėjo, kad Lietuvos Respublikos teisingumo ministro 2025 m. birželio 26 d. įsakymu Nr. 1R-201 „Dėl Nekilnojamojo turto registro informacinės sistemos nuostatų patvirtinimo“ buvo patvirtinti NTR informacinės sistemos nuostatai, kuriuose suteikti įgaliojimai ir įpareigojimai Registrų centrui veikti Teisingumo ministerijos vardu. Pareiga apie įvykusį ADSP informuoti Inspekciją ir duomenų subjektus buvo deleguota Registrų centrui vadovaujantis ADSP valdymo aprašu⁷.

NKSC 2026-10-05 (Inspekcijos reg. Nr. 1R-8104 (2.23 Mr)) Inspekcijai nurodė, kad nagrinėjamo incidento atveju gali būti aktualios trys Informatikos ir ryšių departamentui teiktos rekomendacijos, kurios, NKSC vertinimu, jeigu būtų laiku ir tinkamai įgyvendintos, būtų padėjusios užkirsti kelią ar savalaikiai identifikuoti kibernetinį incidentą. Šios rekomendacijos: 1) iki 2022-12-16 įgalinti tinklę ir tarnybinėse stotyse vykstančių procesų, tinklo komunikacijų stebėjimą, auditavimą ir jų įrašų kaupimą – užtikrinti nuolatinę anomalijų bei kibernetinių incidentų stebėseną. Numatyti nemažesnį kaip 6 mėn. įvykių žurnalų centralizuotą saugojimą; 2) iki 2023-03-16 naudotojų prisijungimams naudoti kelių faktorių autentifikavimą; 3) užtikrinti saugų prisijungimą prie tarnybinio el. pašto, kitų tarnybinių išteklių.

Taikomas teisinis reglamentavimas

BDAR 4 straipsnio 12 punkte įtvirtinta, kad ADSP – tai saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiūsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

BDAR 5 straipsnio 1 dalies f punkte įtvirtintas vientisumo ir konfidencialumo principas įpareigoja duomenų valdytoją duomenis tvarkyti tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

⁵ Ataskaitoje pateikta informacija apie incidento aplinkybes, paveiktas informacines sistemas ir incidento metu taikytas saugumo priemones.

⁶ Informatikos ir ryšių departamentas nurodė negalintis patvirtinti konkretaus būdo, kuriuo buvo perimti naudotojų prisijungimo duomenys.

⁷ Asmens duomenų saugumo pažeidimų valdymo tvarkant asmens duomenis teisės aktais įgaliotiems duomenų tvarkytojams Lietuvos Respublikos teisingumo ministerijos valdomuose registruose ir valstybės informacinėse sistemose tvarkos aprašas, patvirtintas Lietuvos Respublikos teisingumo ministro 2020 m. birželio 25 d. įsakymu Nr. 1R-182 „Dėl asmens duomenų saugumo pažeidimų valdymo tvarkant asmens duomenis teisės aktais įgaliotiems duomenų tvarkytojams Lietuvos Respublikos teisingumo ministerijos valdomuose registruose ir valstybės informacinėse sistemose tvarkos aprašo patvirtinimo“ (toliau – ADSP valdymo aprašas).

Vientisumo ir konfidencialumo principas neatskiriama susijęs su BDAR 24, 32 straipsniuose numatytais prievolėmis duomenų valdytojai įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas tvarkomų asmens duomenų saugumas.

BDAR 24 straipsnio 1 dalyje nustatyta, kad atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrinta ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

BDAR 32 straipsnio 1 dalyje nustatyta, kad atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, *inter alia*, jei reikia: a) pseudonimų suteikimą asmens duomenims ir jų šifravimą; b) gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą; c) gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju; d) reguliarių techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

BDAR 33 straipsnio 1 dalyje nustatyta, kad ADSP atveju duomenų valdytojas nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jis sužino apie ADSP, apie tai praneša priežiūros institucijai, kuri yra kompetentinga pagal 55 straipsnį, nebent ADSP neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms. Jeigu priežiūros institucijai apie ADSP nepranešama per 72 valandas, prie pranešimo pridedamos vėlavimo priežastys. Šio straipsnio 3 dalyje nustatyta, kad pranešime apie ADSP turi būti bent: a) aprašytas ADSP pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijas ir apytikslį skaičių, taip pat atitinkamų asmens duomenų įrašų kategorijas ir apytikslį skaičių; b) nurodyta duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys; c) aprašytos tikėtinos ADSP pasekmės; d) aprašytos priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas ADSP, įskaitant, kai tinkama, priemonės galimoms neigiamoms jo pasekmėms sumažinti. Šio straipsnio 4 dalyje nustatyta, kad kai ir jeigu informacijos neįmanoma pateikti tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais.

BDAR 34 straipsnio 1 dalyje nustatyta, kad kai dėl ADSP gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas praneša apie ADSP duomenų subjektui, o 2 dalyje – kad šio straipsnio 1 dalyje nurodytame pranešime duomenų subjektui aiškia ir paprasta kalba aprašomas ADSP pobūdis ir pateikiama bent 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija ir priemonės.

BDAR preambulės 75 punkte paaiškinta, kad įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms gali kilti dėl tokio asmens duomenų tvarkymo, kurio metu galėtų būti padarytas kūno sužalojimas, materialinė ar nematerialinė žala, visų pirma kai dėl tvarkymo gali kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas, neleistinai panaikinti pseudonimai arba padaryta kita didelė ekonominė ar socialinė žala; kai duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir laisvėmis ar jiems užkertamas kelias kontroliuoti savo asmens duomenis; kai tvarkomi asmens duomenys, kurie atskleidžia rasinę arba etninę kilmę, politines pažiūras, religiją ar filosofinius įsitikinimus, priklausymą profesinėms sąjungoms, taip pat tvarkant genetinius duomenis, sveikatos duomenis ar duomenis apie lytinį gyvenimą, arba apkaltinamuosius nuosprendžius ir nusikalstamas veikas, arba susijusias saugumo priemones; kai siekiant sukurti arba naudoti asmens profilį vertinami asmeniniai aspektai, visų pirma

nagrinėjami arba numatomi su asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu susiję aspektai; kai tvarkomi pažeidžiamų fizinių asmenų, visų pirma vaikų, asmens duomenys; arba kai duomenų tvarkymas apima didelį kiekį asmens duomenų ir daro poveikį daugeliui duomenų subjektų.

BDAR preambulės 83 punkte paaiškinta, kad siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones, pavyzdžiui, šifravimą. Šiomis priemonėmis turėtų būti užtikrintas tinkamo lygio saugumas, įskaitant konfidencialumą, atsižvelgiant į techninių galimybių išsivystymo lygį ir įgyvendinimo sąnaudas pavojų ir saugotinių asmens duomenų pobūdžio atžvilgiu.

BDAR preambulės 86 punkte paaiškinta, kad duomenų valdytojas nepagrįstai nedelsdamas turėtų pranešti duomenų subjektui apie ADSP, kai dėl to ADSP gali kilti didelis pavojus fizinio asmens teisėms ir laisvėms, kad jis galėtų imtis reikiamų priemonių užkirsti tam kelią. Pranešime turėtų būti aprašytas ADSP pobūdis ir pateiktos atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip sumažinti galimą neigiamą poveikį. Tokie pranešimai duomenų subjektams turėtų būti pateikti kuo greičiau ir glaudžiai bendradarbiaujant su priežiūros institucija, laikantis jos ar kitų atitinkamų valdžios institucijų, tokių kaip teisėsaugos institucijos, pateiktų nurodymų. Pavyzdžiui, siekiant sumažinti tiesioginį žalos pavojų, reikėtų nedelsiant apie tai pranešti duomenų subjektams, o ilgesnį pranešimo terminą būtų galima pateisinti būtinybe įgyvendinti tinkamas priemones, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiams ADSP.

Pažymėtina, kad BDAR nenustato detalių saugumo reikalavimų, todėl vertinant duomenų valdytojo taikomas saugumo priemones asmens duomenų saugumui užtikrinti, remiamasi ne tik BDAR, bet ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) metodinėmis rekomendacijomis dėl duomenų saugumo bei atitinkamais saugumo (ISO/IEC) standartais. Be to, Inspekcija, remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.) ir ISO standartais LST ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ bei ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“ yra parengusi ir Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires (toliau – VDAI gairės)⁸ duomenų valdytojams ir duomenų tvarkytojams.

Inspekcijos išvados⁹

Dėl Informatikos ir ryšių departamento

Atlikdama tyrimą Informatikos ir ryšių departamento atžvilgiu Inspekcija vertino, ar pastarasis, prieš įvykstant ADSP, ėmėsi tinkamų techninių ir organizacinių priemonių, kad tokie ADSP neįvyktų, taip pat veiksmai ir priemonės, kurių Informatikos ir ryšių departamentas ėmėsi įvykus ADSP.

Nuostatų¹⁰ 9.1 papunktyje nustatyta, kad vienas iš Informatikos ir ryšių departamento veiklos tikslų yra užtikrinti vidaus reikalų ministrui pavestose valdymo srityse naudojamų registru

⁸ Prie VDAI gairėse nurodytų priemonių yra pateikiamos nuorodos į susijusį informacijos saugumo valdymo standarto LST ISO/IEC 27001:2017 reikalavimą ir jį papildantį privatumo užtikrinimo reikalavimą pagal ISO/IEC 27701:2019.

⁹ Pagal Inspekcijos informacinių technologijų skyriaus 2026-10-14 tikrinimo ataskaitą Nr. 4R-626 (2.14 E) „Dėl Migracijos departamento prie Lietuvos Respublikos Vidaus reikalų ministerijos asmens duomenų saugumo pažeidimo“.

¹⁰ Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos nuostatai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2002 m. rugsėjo 13 d. įsakymu Nr. 439 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos nuostatų patvirtinimo“ (toliau – Nuostatai).

informacinių sistemų ir valstybės informacinių sistemų kūrimą, tvarkymą, plėtrą, saugą, <...>. Nuostatų 10.7 papunktyje nustatyta, jog Informatikos ir ryšių departamentas užtikrina tinkamas technines priemones, kad duomenų tvarkymas Vidaus reikalų ministerijos valdomose ir Informatikos ir ryšių departamento tvarkomose registru informacinėse sistemose ir valstybės informacinėse sistemose atitiktų įstatymų ir kitų teisės aktų, reglamentuojančių valstybės informacinių išteklių tvarkymą, informacijos saugą, kibernetinį saugumą, reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Taip pat Nuostatų 10.15 papunktyje nustatyta, kad Informatikos ir ryšių departamentas tvarko jo informacinių išteklių infrastruktūroje veikiančias Vidaus reikalų ministerijos administracijos padalinių, įstaigų prie Vidaus reikalų ministerijos ir kitų vidaus reikalų ministrui pavestų valdymo sričių įstaigų el. pašto, incidentų ir paslaugų valdymo bei kitas bendrojo naudojimo informacines sistemas ir informacinių technologijų sprendinius.

Tyrimo metu nustatyta, kad Informatikos ir ryšių departamentas ir Migracijos departamentas yra sudarę informacinių technologijų ir telekomunikacijų paslaugų teikimo 2019-05-27 sutartį (paslaugų lygio susitarimą) Nr. 15R-136 (toliau – Paslaugų sutartis), kurios priede (Paslaugų specifikacija) yra nurodoma, kad Informatikos ir ryšių departamentas teikia Migracijos departamentui tarnybinio el. pašto paslaugas.

Atsižvelgiant į minėtas Nuostatų ir Paslaugų sutarties nuostatas konstatuotina, kad Informatikos ir ryšių departamentas ADSP metu buvo atsakingas už el. pašto sistemos, kuria ADSP metu naudojosi Migracijos departamentas, administravimą, priežiūrą ir saugos užtikrinimą, todėl jam kilo pareiga įgyvendinti tinkamas technines ir organizacines priemones, skirtas užtikrinti šios sistemos saugumą bei savalaikį reagavimą į galimus saugumo incidentus.

Pagal BDAR 32 straipsnio 1 dalį tiek duomenų valdytojas, tiek duomenų tvarkytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, užtikrinančias pavojaus atitinkantį saugumo lygį. Vertinant Informatikos ir ryšių departamento vaidmenį nagrinėjamu atveju, reikšmingas ne vien formalus jo įvardijimas, bet ir faktiškai vykdytos funkcijos bei atsakomybės.

Nuostatų 10.1 papunktyje nustatyta, kad Informatikos ir ryšių departamentas vykdo Vidaus reikalų ministerijos valdomų ir departamento tvarkomų registru informacinių sistemų bei valstybės informacinių sistemų tvarkytojo funkcijas, o pirmiau minėtame 10.15 papunktyje – kad tvarko jo informacinių išteklių infrastruktūroje veikiančias Vidaus reikalų ministerijos administracijos padalinių, įstaigų prie Vidaus reikalų ministerijos ir kitų vidaus reikalų ministrui pavestų valdymo sričių įstaigų el. pašto, incidentų ir paslaugų valdymo bei kitas bendrojo naudojimo informacines sistemas ir informacinių technologijų sprendinius. Be to, tyrimo metu nustatyta, kad Informatikos ir ryšių departamentas administravo ADSP metu paveiktą Microsoft Exchange Server 2019 sistemą, buvo atsakingas už jos techninę priežiūrą ir saugumo priemonių įgyvendinimą.

Atsižvelgiant į tai, kad Informatikos ir ryšių departamentas pagal jam pavestas funkcijas ir Paslaugų sutartį administravo Migracijos departamento naudojamą el. pašto sistemą, vykdė jos techninę priežiūrą, užtikrino veikimą ir saugumą, tačiau pats nenustatė asmens duomenų tvarkymo tikslų, darytina išvada, kad Informatikos ir ryšių departamentas veikė kaip duomenų tvarkytojas BDAR 4 straipsnio 8 punkto prasme. Todėl jam tiesiogiai taikoma BDAR 32 straipsnio 1 dalyje nustatyta pareiga įgyvendinti tinkamas technines ir organizacines priemones, užtikrinančias pavojaus atitinkantį asmens duomenų saugumo lygį.

Kibernetinio saugumo reikalavimų aprašo¹¹ XII skirsnio „Prieigos valdymas ir kelių veiksmų tapatumo nustatymo priemonės“ 7 lentelės 61 punkte nustatyta, kad naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksmų tapatumo nustatymo priemonės).

¹¹ Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 (toliau – Kibernetinio saugumo reikalavimų aprašas).

ISO standarto¹² 8.5 papunktyje „Saugus autentiškumo patvirtinimas“ nustatyta, kad turėtų būti pasirinktas tinkamas autentiškumo patvirtinimo metodas, o 8.3 papunktyje „Prieigos prie informacijos ribojimas“ nustatyta, kad turi būti užkertamas kelias neleistinai prieigai, atsižvelgiant į prieigos leidimų suteikimą pagal tapatybę, įtaisą, vietą ar taikomąją programą.

VDAI gairių 91 punkte nustatyta, kad <...> kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė <...>.

Atsižvelgiant į nurodytas Kibernetinio saugumo reikalavimų aprašo, ISO standarto ir VDAI gairių nuostatas konstatuotina, jog siekiant užtikrinti asmens duomenų saugumą turi būti pasirinkti tinkami autentiškumo patvirtinimo metodai (pvz., kelių faktorių autentifikaciją (MFA) ir / ar leidimą jungtis prie sistemų tik iš žinomų IP adresų, iš tam tikrų LAN tinklų, iš tam tikros teritorijos ar kt.).

Informatikos ir ryšių departamentas atsakyme Inspekcijai paaiškino, jog pirmiau nurodytos techninės priemonės ADSP metu nebuvo taikomos, kadangi Kibernetinio saugumo reikalavimų apraše nurodyti techniniai reikalavimai privalo būti įgyvendinti ne vėliau kaip per 24 mėnesius nuo Informatikos ir ryšių departamento įregistravimo Kibernetinio saugumo informacinėje sistemoje dienos, t. y. iki 2027-04-17.

Inspekcija pažymi, jog saugumo reikalavimai yra nustatyti ne tik Kibernetinio saugumo reikalavimų apraše. BDAR preambulės 78 punkte, be kita ko, numatyta, jog siekiant užtikrinti fizinių asmenų teisių ir laisvių apsaugą tvarkant asmens duomenis reikia imtis tinkamų techninių ir organizacinių priemonių siekiant užtikrinti, kad būtų laikomasi šio reglamento reikalavimų. Kad galėtų įrodyti, jog laikosi šio reglamento, duomenų valdytojas turėtų priimti vidaus nuostatas ir įgyvendinti priemones, kuriomis visų pirma būtų paisoma pritaikytosios ir standartizuotosios duomenų apsaugos principų.

BDAR nenustato detalių saugumo reikalavimų, todėl vertinant taikomas saugumo priemones asmens duomenų saugumui užtikrinti turi būti remiamasi ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) metodinėmis rekomendacijomis dėl duomenų saugumo bei atitinkamais saugumo (ISO) standartais. Remiantis vieša Lietuvos akreditacijos ir standartizacijos agentūros informacija, ISO standarte pateikiamas bendrųjų informacijos saugumo kontrolės priemonių informacinis rinkinys, įskaitant įgyvendinimo nurodymus. Šis standartas skirtas naudoti organizacijoms: a) informacijos saugumo valdymo sistemos (ISVS), pagrįstos ISO/IEC 27001, kontekste; b) įgyvendinant tarptautiniu mastu pripažinta geriausia praktika pagrįstas informacijos saugumo kontrolės priemones; c) rengiant konkrečios organizacijos informacijos saugumo kontrolės gaires.

Regionų administracinis teismas 2026-05-06 sprendime administracinėje byloje Nr. eI3-1654-422/2026 pažymėjo, kad ISO standarte būtent ir yra įtvirtinti Europos Sąjungoje taikomi informacijos saugumo, kibernetinio saugumo ir privatumo apsaugos principai. Taip pat teismas pažymėjo, kad VDAI gairės parengtos remiantis ISO standartais, kuriais nustatyti Informacinių technologijų saugumo užtikrinimo metodai ir metodika saugumo pažeidimų nustatymui.

Atsižvelgiant į tai, kas nurodyta, Inspekcija sprendžia, kad Informatikos ir ryšių departamento nurodyta aplinkybė, jog pirmiau minėtos techninės priemonės nebuvo taikomos, kadangi Kibernetinio saugumo reikalavimų apraše nurodyti techniniai reikalavimai ADSP metu neprivalėjo būti įgyvendinami, nagrinėjamu atveju reikšmės neturi, kadangi ne tik minėtas aprašas, bet, pirmiausia, BDAR įpareigoja įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, o ISO standarte ir VDAI gairėse, kurie buvo aktualūs ir viešai paskelbti iki įvykstant ADSP, yra nustatyti saugumo principai ir jų įgyvendinimo būdai.

¹² ISO/IEC 27002:2022 standartas „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (toliau – ISO standartas).

Tyrimo metu nustatyta, kad Migracijos departamento darbuotojai galėjo pasiekti Microsoft Exchange Server 2019 sistemą per naršyklę, adresu [DUOMENYS NESKELBTINI], o prisijungimams nebuvo taikomi papildomi saugumo apribojimai (pvz., MFA ar prieigos ribojimas pagal vietą, įrenginį ar sąlygines prieigos taisykles).

Inspekcija pažymi, jog tretiesiems asmenims pavyko prisijungti prie dviejų Informatikos ir ryšių departamento administruojamų Migracijos departamento naudojamų el. pašto paskyrų, prie kurių buvo galima jungtis ne iš Migracijos departamento vidinio tinklo, naudojant Migracijos departamento darbuotojų prisijungimo vardus ir slaptažodžius, tačiau jei naudojantis naršykle ir jungiantis prie el. pašto paskyrų būtų taikoma MFA ar įdiegtas prieigos ribojimas tik įgaliojams asmenims (pvz., pagal iš anksto nurodytus IP adresus arba tik iš tam tikros teritorijos), tretieji asmenys nebūtų neteisėtai prisijungę prie paveiktų el. pašto paskyrų ir ADSP nebūtų įvykęs. Pažymėtina, kad jungiantis prie sistemų su MFA, atlikus pirmą žingsnį (įvedus prisijungimo vardą ir slaptažodį), toliau yra inicijuojamas antras žingsnis (autentifikavimas) į iš anksto nustatytą priemonę išsiunčiant prisijungimo kodą arba naudojantis papildomomis autentifikavimo programėlėmis (pvz., mobiliojo telefono programėle), kuriose yra generuojamas laikinas kodas. Atitinkamai, nagrinėjamu atveju antras žingsnis nebūtų atliktas net tretiesiems asmenims žinant ar atspėjus prisijungimo vardą ir slaptažodį. Be to, taikant sistemų pasiekimo ribojimą pagal IP adresus ar iš anksto nustatytą teritoriją, net ir žinant ar atspėjus prisijungimo vardą ir slaptažodį, prie sistemų nebūtų galima prisijungti, kadangi sistema nebūtų pasiekama, nes tretieji asmenys dar papildomai turėtų patekti į vidinį Migracijos departamento tinklą, gauti prieigą pagal IP adresą arba būti tam tikroje teritorijoje.

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad ADSP metu Informatikos ir ryšių departamento prižiūrime el. pašto sistemoje nebuvo užtikrinamas tinkamas asmens duomenų saugumo lygis, kadangi nebuvo taikomas MFA ar įdiegtas prieigos ribojimas tik įgaliojams asmenims (pvz., pagal iš anksto nurodytus IP adresus arba tik iš tam tikros teritorijos).

Kibernetinio saugumo reikalavimų aprašo VII skirsnio „Tinklų ir informacinių sistemų įsigijimas, plėtojimas ir priežiūros saugumas, įskaitant spragų valdymą ir atskleidimą“ 3 lentelės 30 punkte nurodyta, kad turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai.

ISO standarto 8.8 papunktyje „Techninių pažeidžiamumų valdymas“ nurodyta, kad turėtų būti įdiegtas programinės įrangos atnaujinimo valdymo procesas tam, kad būtų užtikrinta, jog visoje leidžiamoje programinėje įrangoje būtų įdiegtos naujausios patvirtintos pataisos ir programų atnaujinimai.

VDAI gairių 97 punkte nurodyta, kad kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

Atsižvelgiant į nurodytas Kibernetinio saugumo reikalavimų aprašo, ISO standarto ir VDAI gairių nuostatas konstatuotina, jog siekiant užtikrinti asmens duomenų saugumą asmens duomenims tvarkyti naudojamos informacinės sistemos programinė įranga turi būti tinkamai prižiūrima, o nustatytiems pažeidžiamumams šalinti turi būti laiku diegiamos gamintojo teikiamos saugumo pataisos ir programinės įrangos atnaujinimai.

Tyrimo metu nustatyta, kad Migracijos departamento elektroninio pašto paslaugoms teikti buvo naudojama Informatikos ir ryšių departamento administruojama Microsoft Exchange Server 2019 sistema, kuri buvo pasiekama ne tik iš Migracijos departamento vidinio tinklo, bet ir per išorinį tinklą pasiekiamą adresą [DUOMENYS NESKELBTINI]. Taip pat tyrimo metu nustatyta, kad Microsoft Exchange Server 2019 sistemos gamintojo palaikymas baigėsi 2025-10-14, todėl po šios datos naudojamai sistemai gamintojas nebeteikė įprastų techninio palaikymo paslaugų, įskaitant klaidų ir saugumo pažeidžiamumų pataisas. Pažymėtina, kad sistemos, kuriai nebeteikiamos saugumo pataisos, tolesnis naudojimas, ypač kai ši sistema yra pasiekama ne tik iš vidinio tinklo, neužtikrina tinkamo su techniniais pažeidžiamumais susijusios rizikos valdymo, nes naujai nustatyti

pažeidžiamumai gali likti neištaisyti ir būti išnaudoti neteisėtai prieigai prie sistemos bei joje tvarkomų asmens duomenų gauti. Atsižvelgiant į tai spręstina, jog Microsoft Exchange Server 2019 sistemos eksploatavimas po gamintojo palaikymo pabaigos neatitiko reikalavimo įgyvendinti tinkamas technines ir organizacines priemones, skirtas užtikrinti tvarkymo saugumą, atsižvelgiant į tvarkymui kylančią riziką, tačiau kartu pažymėtina, kad tyrimo metu nenustatyta duomenų, jog ši aplinkybė turėjo įtakos nagrinėjamo ADSP kilimui ar jo eigai.

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad Informatikos ir ryšių departamento prižiūrime el. pašto sistemoje nebuvo užtikrinamas tinkamas asmens duomenų saugumo lygis, kadangi buvo naudojama gamintojo nebepalaikoma Microsoft Exchange Server 2019 sistema.

ISO standarto 5.26 papunktyje „Reagavimas į informacijos saugumo incidentus“ nustatyta, kad organizacija iš anksto turi nusistatyti reagavimo į informacijos saugumo incidentus procedūras ir reaguojant į juos vadovautis nustatytomis procedūromis, taip pat informuoti visas susijusias suinteresuotas šalis.

Atsižvelgiant į nurodytą ISO standarto nuostatą, duomenų valdytojai ir duomenų tvarkytojai privalo reaguoti į informacijos saugumo incidentus pagal nustatytas procedūras, siekiant nustatyti incidento pobūdį, mastą, poveikį ir imtis priemonių jo pasekmėms suvaldyti. Reagavimas į incidentą apima ne tik pirminių požymių identifikavimą, bet ir jų tyrimą, siekiant nustatyti, ar buvo įvykdyta neteisėta prieiga prie informacinių išteklių, kokie duomenys galėjo būti paveikti ir kokių veiksmų reikia imtis siekiant užkirsti kelią tolesnei žalai. Taip pat duomenų valdytojai ir duomenų tvarkytojai, nustatę ADSP priežastis, privalo imtis priemonių, kurios užtikrintų, kad poveikis duomenų subjektams būtų sumažintas, ADSP būtų sustabdytas ir ateityje tokie ADSP nepasikartotų.

[DUOMENYS NESKELBTINI]¹³.

Tyrimo metu nustatyta, kad Informatikos ir ryšių departamentas disponavo informacija apie netipinius prisijungimus ir galimą Migracijos departamento darbuotojų el. pašto paskyrų kompromitavimą. Taip pat nustatyta, kad gavęs šią informaciją neatliko pakankamų veiksmų (įskaitant išsamią žurnalinių įrašų analizę), kad įvertintų, ar tretiesiems asmenims pavyko neteisėtai prisijungti prie Migracijos departamento darbuotojų el. pašto paskyrų, ar buvo peržiūrėtas jų turinys, ar atlikti kiti veiksmai, rodantys neteisėtą prieigą prie informacijos.

Pažymėtina, jog Informatikos ir ryšių departamentas, kaip esantis atsakingas už el. pašto sistemos, kuria ADSP metu naudojosi Migracijos departamentas, administravimą, priežiūrą ir saugos užtikrinimą, gavęs informaciją apie galimą neteisėtą prieigą prie el. pašto paskyrų, privalėjo nedelsdamas pradėti incidento tyrimą ir nustatęs galimą ADSP informuoti Migracijos departamentą. Informatikos ir ryšių departamentui neatlikus incidento tyrimo, nenustačius incidento priežasčių ir jo masto, neidentifikavus galimai pažeistų ar neteisėtai panaudotų naudotojų paskyrų, neįvertinus su incidentu susijusių sistemų žurnalinių įrašų ir nenustačius, ar pažeidžiamumai, sudarę sąlygas neteisėtai prieigai, tebėra sistemoje ir gali būti toliau išnaudojami, nebuvo užkirstas kelias atliktiems neteisėtiems prisijungimams prie NTR ir JAR slaptažodžių atnaujinimams, todėl tretiesiems asmenims pavyko neteisėtai prisijungti ne tik prie el. pašto paskyrų, bet ir prie NTR ir JAR. Dėl šios priežasties ADSP tęsėsi ilgą laiką, t. y. nuo 2026-01-06 iki 2026-04-02, o paveiktų asmens duomenų ir duomenų subjektų apimtis yra itin didelė.

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad Informatikos ir ryšių departamentas, gavęs informaciją apie galimą paskyrų kompromitavimą, neįvertino, ar saugumo incidento metu buvo gauta neteisėta prieiga prie Migracijos departamento darbuotojų el. pašto paskyrų ir ar dėl to galėjo būti pažeistas asmens duomenų konfidencialumas. Dėl neatlikto vertinimo nebuvo laiku nustatytas ADSP ir nedelsiant informuotas Migracijos departamentas.

¹³ Tyrimo metu nustatyta, kad Informatikos ir ryšių departamentas disponavo informacija apie netipinius prisijungimus ir galimą paskyrų kompromitavimą, tačiau neatliko pakankamų veiksmų siekdamas įvertinti, ar buvo gauta neteisėta prieiga prie paskyrų ir jose tvarkomų asmens duomenų.

Pažymėtina, kad, atsižvelgiant į pirmiau nurodytą NKSC pateiktą informaciją (žr. sprendimą dalyje „Inspekcijai pateikta informacija“), Informatikos ir ryšių departamentas apie saugumo spragas ir nepakankamą techninių ir organizacinių priemonių taikymą / netaikymą žinojo iki įvykstant ADSP, tačiau saugumo spragų nepašalino ir tinkamų techninių ir organizacinių priemonių laiku bei tinkamai neįgyvendino.

Apibendrinant tyrimo metu nustatytą informaciją konstatuotina, kad ADSP įvyko dėl Informatikos ir ryšių departamento nepakankamai užtikrintos prieigų kontrolės ir autentifikavimo priemonių taikymo, kadangi jungiantis prie Microsoft Exchange Server 2019 sistemos, kuri buvo viešai pasiekama adresu [DUOMENYS NESKELBTINI], nebuvo taikomas MFA, taip pat nebuvo įdiegtos papildomos prieigos kontrolės priemonės, užtikrinančios prieigą tik įgaliojusiems asmenims. Taip pat Informatikos ir ryšių departamentas, nustatęs galimą Migracijos departamento el. pašto paskyrų kompromitavimą, tinkamai neįvertino, ar saugumo incidento metu buvo gauta neteisėta prieiga prie Migracijos departamento darbuotojų el. pašto paskyrų ir ar dėl to galėjo būti pažeistas asmens duomenų konfidencialumas. Be to, ADSP metu Informatikos ir ryšių departamento prižiūrime el. pašto sistemoje buvo naudojama gamintojo nebepalaikoma Microsoft Exchange Server 2019 sistema, nors tyrimo metu ir nenustatyta, kad ši aplinkybė turėjo įtakos nagrinėjamo ADSP kilimui ar jo eigai.

Remiantis tuo, kas nurodyta, darytina išvada, jog Informatikos ir ryšių departamentas savo veiksmais (neveikimu) netinkamai įgyvendino ISO standarto 5.26, 8.3, 8.5 ir 8.8 papunkčių reikalavimus ir tokiu būdu pažeidė BDAR 5 straipsnio 1 dalies f punkte įtvirtintą konfidencialumo principą ir BDAR 32 straipsnio 1 dalies b punktą.

Įvykus ADSP Informatikos ir ryšių departamentas [DUOMENYS NESKELBTINI].

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad įvykus ADSP Informatikos ir ryšių departamentas ėmėsi reikiamų veiksmų.

Dėl Migracijos departamento

Atlikdama tyrimą Migracijos departamento atžvilgiu Inspekcija vertino, ar pastarasis, prieš įvykstant ADSP, ėmėsi tinkamų techninių ir organizacinių priemonių, kad toks ADSP neįvyktų, taip pat veiksmai ir priemonės, kurių Migracijos departamentas ėmėsi įvykus ADSP.

Migracijos departamentas, atsižvelgiant į sudarytas duomenų teikimo sutartis ir papildomus susitarimus, yra NTR ir JAR duomenų gavėjas, ir šiuo aspektu veikia kaip duomenų valdytojas (BDAR 4 straipsnio 7 punktas), kadangi būtent jis nustato, kuriems darbuotojams ir kokių tikslu turi būti suteikta prieiga prie NTR ir JAR, bei kontroliuoja tokių prieigų naudojimą. Atsižvelgiant į tai, Migracijos departamentas, kaip duomenų valdytojas, turi pareigą įvertinti prieigos suteikimui reikšmingas aplinkybes ir pateikti Registrų centrui informaciją, būtiną tinkamoms prieigos kontrolės priemonėms įgyvendinti.

Pagal BDAR 24 straipsnio 1 dalį duomenų valdytojas, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento, tos priemonės prireikus peržiūrimos ir atnaujinamos.

ISO standarto 8.3 papunktyje „Prieigos prie informacijos ribojimas“ nustatyta, kad turi būti užkertamas kelias neleistinai prieigai, atsižvelgiant į prieigos leidimų suteikimą pagal tapatybę, įtaisą, vietą ar taikomąją programą.

VDAI gairių 91 punkte nustatyta, kad <...> kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė <...>.

Atsižvelgiant į šias nuostatas, duomenų valdytojas, siekdamas užtikrinti asmens duomenų saugumą, privalo pasirinkti tinkamus autentiškumo patvirtinimo metodus (pvz., MFA ir / ar leidimą jungtis prie sistemų tik iš žinomų IP adresų, iš tam tikrų LAN tinklų, iš tam tikros teritorijos ar kt.).

Migracijos departamentas atsakyme Inspekcijai nurodė, kad darbuotojų prieigų suteikimo ar panaikinimo atveju raštu Registrų centrui pateikia darbuotojo vardą, pavardę, asmens kodą ir tarnybinio el. pašto adresą, IP adresai yra nurodyti NTR 2013 sutarties 2 priede ir JAR 2017 sutarties 3 priede.

Pažymėtina, kad NTR 2013 sutarties 1 priedo „Duomenys ir jų teikimo sąlygos“ 6.1 papunktyje nurodyta, kad gavėjas sutarties 2 priede pateikia išorinį (-ius) IP adresą (-us), iš kurio (-ių) bus kreipiamasi į teikėjo duomenų banką, nurodydamas duomenų naudotojus. JAR 2017 sutarties 2020-04-20 Susitarimo¹⁴ 16 priedo „Juridinių asmenų registro duomenų teikimo ir naudojimo sąlygos (WEB priemonėmis)“ 5.1 papunktyje nurodyta, kad gavėjas JAR 2017 sutarties 20 priede pateikia išorinį (-ius) IP adresą (-us), iš kurio (-ių) bus kreipiamasi į teikėjo duomenų banką, nurodydamas duomenų naudotojus. Tyrimo medžiagoje esančios NTR 2013 sutarties 2 priede „Duomenų naudotojų sąrašas“ prie kiekvieno Migracijos departamento įrašyto darbuotojo yra nurodytas naudotojo vardas, pavardė, asmens kodas, pareigos, telefonas ir el. pašto adresas, faksas ir išorinis IP adresas, iš kurio naudotojas jungsis prie NTR. Taip pat JAR 2017 sutarties 2020-04-20 Susitarimo 20 priede „Duomenų vartotojų sąrašas“, teikiant duomenis pagal JAR 2017 sutarties 2020-04-20 Susitarimo 16 priedą, Migracijos departamentas turi nurodyti kiekvieno naudotojo vardą, pavardę, pareigas, telefoną, el. pašto adresą ir konkretų išorinį IP adresą.

Atsižvelgiant į tai, Migracijos departamentas, kaip duomenų valdytojas, papildydamas duomenų naudotojų sąrašus pagal NTR 2013 sutartį ir JAR 2017 sutartį, prie kiekvieno naudotojo turi nurodyti išorinį (-ius) IP adresą (-us), iš kurio bus jungiamasi prie NTR ir JAR.

Tyrimo metu Registrų centras pateikė Migracijos departamento 2021-02-01 ir 2023-07-12 raštus dėl JADIS / JARIS, NTR ir GR naudotojų sąrašų atnaujinimo, kuriais prašė Registrų centro į sąrašus įtraukti dvi darbuotojas, kurių paskyros buvo paveiktos ADSP metu. Prašymuose Migracijos departamentas nurodė naujų naudotojų vardus ir pavardes, asmens kodus ir el. pašto adresus, tačiau išorinių IP adresų nenurodė. Migracijos departamentas atsakyme Inspekcijai paaiškino, jog IP adresai, kuriais Registrų centras galėjo leisti naudotis NTR ir JAR, buvo nurodyti pirmiau minėtuose NTR 2013 sutarties bei JAR 2017 sutarties (ir 2020-04-20 Susitarimo) prieduose, tačiau, pažymėtina, kad Migracijos departamento lūkestis, jog sutartyse nurodyti IP adresai bus taikomi visiems ateityje teikiamiems prašymams, laikytinas nepagrįstu. Atkreiptinas dėmesys, kad nesant aiškaus susitarimo dėl tokių IP adresų taikymo ateityje (o tokio susitarimo nei NTR 2013 sutartyje, nei JAR 2017 sutartyje ir papildomuose susitarimuose bei jų prieduose nebuvo), Migracijos departamentas, kiekvieną kartą kreipdamasis dėl naujo naudotojo sukūrimo ir prieigos prie registrų jam suteikimo, turėjo nurodyti konkretų IP adresą (adresus), iš kurių bus jungiamasi prie registrų.

Papildomai pažymėtina, kad tretiesiems asmenims pavyko prisijungti prie NTR ir JAR prisijungus prie Migracijos departamento el. pašto paskyrų ir pakeitus prisijungimo prie NTR ir JAR slaptažodžius. Jei Migracijos departamentas prašymuose atnaujinti duomenų naudotojų sąrašus būtų nurodęs naudotojui taikomus išorinius IP adresus, Registrų centras būtų šiems vartotojams taikęs apribojimus pagal nurodytus IP adresus. Tačiau, pabrėžtina, nors Migracijos departamentas, teikdamas prašymus dėl naudotojų įtraukimo į NTR ir JAR duomenų naudotojų sąrašus ir nenurodydamas konkrečių išorinių IP adresų, nesiėmė visų priemonių, kurios galėjo sumažinti

¹⁴ Susitarimas dėl JAR 2017 sutarties pakeitimo (toliau – JAR 2017 sutarties 2020-04-20 Susitarimas).

neteisėtos prieigos prie sistemų riziką, vertinama, kad vien IP adresų nenurodymas savaime nesukūrė galimybės tretiesiems asmenims gauti prieigą prie asmens duomenų (NTR ir JAR).

Apibendrinant tyrimo metu nustatytą informaciją konstatuotina, kad Migracijos departamentas, teikdamas prašymus Registrų centrui dėl naudotojų įtraukimo į NTR ir JAR duomenų naudotojų sąrašus ir nenurodydamas konkrečių išorinių IP adresų, nesiėmė visų priemonių, kurios galėjo sumažinti neteisėtos prieigos prie sistemų riziką, tačiau vien išorinių IP adresų nenurodymas savaime nesukūrė galimybės tretiesiems asmenims gauti prieigą prie asmens duomenų.

Remiantis tuo, kas nurodyta, darytina išvada, jog Migracijos departamentas savo veiksmais (neveikimu) netinkamai įgyvendino ISO standarto 8.3 papunkčio reikalavimus ir tokiu būdu pažeidė BDAR 24 straipsnio 1 dalį.

Įvykus ADSP Migracijos departamentas inicijavo ADSP tyrimą, kurį atliekant bendradarbiavo su Registrų centru ir Informatikos ir ryšių departamentu, siekdamas užtikrinti, kad būtų nustatytos ADSP priežastys ir būtų imtasi priemonių, kad ateityje tokie ADSP nepasikartotų.

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad įvykus ADSP Migracijos departamentas ėmėsi reikiamų veiksmų.

Dėl Registrų centro

Atlikdama tyrimą Registrų centro atžvilgiu Inspekcija vertino, ar pastarasis, prieš įvykstant ADSP, ėmėsi tinkamų techninių ir organizacinių priemonių, kad toks ADSP neįvyktų, taip pat veiksmai ir priemonės, kurių Registrų centras ėmėsi įvykus ADSP.

Dėl techninių ir organizacinių priemonių taikymo

NTR nuostatų¹⁵ 7 ir 8 punktuose nustatyta, kad NTR valdytojas ir NTR tvarkomų asmens duomenų valdytojas yra Teisingumo ministerija, o NTR tvarkytojas ir NTR tvarkomų asmens duomenų tvarkytojas yra Registrų centras.

NTR nuostatų 11.17 papunktyje nustatyta, kad NTR tvarkytojas (Registrų centras) privalo taikyti reikiamas technines ir organizacines priemones, kad būtų užtikrintas asmens duomenų saugumas, konfidencialumas, vientisumas ir prieinamumas, įskaitant apsaugą nuo atsitiktinio ar neteisėto duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo <...>.

JAR nuostatų¹⁶ 10 ir 11 punktuose nustatyta, kad JAR valdytojas, JAR tvarkomų asmens duomenų valdytojas yra Teisingumo ministerija, o JAR tvarkytojas, JAR tvarkomų asmens duomenų tvarkytojas yra Registrų centras.

JAR nuostatų 13.2 papunktyje nustatyta, kad Registrų centras užtikrina duomenų, informacijos ir dokumentų saugą, nustato saugos priemones ir jų vykdymo tvarką, o 13.18 papunktyje – jog taiko reikiamas technines ir organizacines priemones, kad būtų užtikrintas asmens duomenų saugumas, konfidencialumas, vientisumas ir prieinamumas, įskaitant apsaugą nuo atsitiktinio ar neteisėto duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo <...>.

Pagal BDAR 32 straipsnio 1 dalį tiek duomenų valdytojas, tiek duomenų tvarkytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, užtikrinančias pavojų atitinkantį

¹⁵ Nekilnojamojo turto registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2014 m. balandžio 23 d. nutarimu Nr. 379 „dėl Nekilnojamojo turto registro nuostatų patvirtinimo“ (toliau – NTR nuostatai).

¹⁶ Juridinių asmenų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 12 d. nutarimu Nr. 1407 „dėl Juridinių asmenų registro nuostatų patvirtinimo“ (toliau – JAR nuostatai).

saugumo lygį. Atsižvelgiant į pirmiau nurodytą NTR nuostatų ir JAR nuostatų teisinį reglamentavimą, Registrų centras yra atsakingas už NTR ir JAR tvarkomų asmens duomenų saugumą, įskaitant apsaugą nuo atsitiktinio ar neteisėto duomenų atskleidimo, todėl jam kilo pareiga įgyvendinti tinkamas technines ir organizacines priemones, užtikrinančias pavojų atitinkantį saugumo lygį.

Kibernetinio saugumo reikalavimų aprašo 7 lentelės 61 punkte nustatyta, kad naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksmų tapatumo nustatymo priemonės).

ISO standarto 8.3 papunktyje „Prieigos prie informacijos ribojimas“ nustatyta, kad turi būti užkertamas kelias neleistinai prieigai, atsižvelgiant į prieigos leidimų suteikimą pagal tapatybę, įtaisą, vietą ar taikomąją programą, o 8.5 papunktyje „Saugus autentiškumo patvirtinimas“ – kad turėtų būti pasirinktas tinkamas autentiškumo patvirtinimo metodas.

VDAI gairių 91 punkte nustatyta, kad <...> kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adresų kontrolė <...>.

Atsižvelgiant į nurodytas Kibernetinio saugumo reikalavimų aprašo, ISO standarto ir VDAI gairių nuostatas konstatuotina, jog duomenų valdytojas (nagrinėjamu atveju duomenų tvarkytojas), siekdamas užtikrinti asmens duomenų saugumą, privalo pasirinkti tinkamus autentiškumo patvirtinimo metodus (pvz., kelių faktorių autentifikaciją (MFA) ir / ar leidimą jungtis prie sistemų tik iš žinomų IP adresų, iš tam tikrų LAN tinklų, iš tam tikros teritorijos ar kt.).

Tyrimo metu, vertinant Registrų centro pateiktą informaciją, nustatyta, jog ADSP metu jungimuisi prie NTR ir JAR nebuvo naudojamas MFA, taip pat naudotojams, kurių prisijungimo duomenys buvo paveikti, nebuvo taikomas IP filtravimas.

Pažymėtina, kad jungiantis prie sistemų su MFA, atlikus pirmą žingsnį (įvedus prisijungimo vardą ir slaptažodį), toliau yra inicijuojamas antras žingsnis (autentifikuojamas) į iš anksto nustatytą priemonę išsiunčiant prisijungimo kodą arba naudojantis papildomomis autentifikavimo programėlėmis (pvz., mobiliojo telefono programėle), kuriose yra generuojamas laikinas kodas. Atitinkamai nagrinėjamu atveju antras žingsnis nebūtų atliktas net tretiesiems asmenims iš anksto žinant prisijungimo vardą ir slaptažodį. Be to, taikant sistemos pasiekimo ribojimą pagal IP adresus ar iš anksto nustatytą teritoriją, net ir žinant prisijungimo vardą ir slaptažodį, prie sistemos nebūtų galima prisijungti, kadangi sistema nebūtų pasiekama, nes tretieji asmenys dar papildomai turėtų pateikti į vidinį Migracijos departamento tinklą, gauti prieigą pagal IP adresą arba būti tam tikroje teritorijoje.

Atkreiptinas dėmesys, kad Registrų centras Migracijos departamentui NTR ir JAR duomenis teikė NTR 2013 sutarties ir JAR 2017 sutarties pagrindu.

JAR 2017 sutarties 2020-04-20 Susitarimo 16 priedo 5.1 papunktyje nustatyta, kad gavėjas pateikia išorinį (-ius) IP adresą (-us), iš kurio(-ių) bus kreipiamasi į teikėjo duomenų banką, nurodydamas duomenų naudotojus. 6.2 papunktyje nurodyta, kad tuomet paslaugų gavėjas turi teisę naudotis duomenų teikimo sistema iš naudotojų sąrašė nurodyto (-ų) išorinio (-ų) IP adresų (-ų), o Registrų centras, pastebėjęs, kad paslaugų gavėjas su jam suteiktu naudotojo vardu ir slaptažodžiu peržiūri duomenis ne iš nurodyto išorinio IP adresų, neleidžia jam naudotis duomenų teikimo sistema; jei išorinis IP adresas nėra nurodytas, paslaugų gavėjui yra leidžiama naudotis duomenų teikimo sistema, kreipiantis iš bet kurio IP adresų.

NTR 2013 sutarties 1 priedo 7.3 papunktyje įtvirtintas reikalavimas, kad Migracijos departamentas, teikdamas prašymus dėl naujo naudotojo, turi nurodyti išorinius IP adresus, kitu atveju Registrų centras turi neleisti jungtis prie NTR. Atsižvelgiant į tai, Registrų centras turi užtikrinti, kad prie NTR naudotojai nesijungtų iš nepatvirtintų IP adresų.

Registrų centras atsakyme nurodė, kad Migracijos departamentas teikė 2021-02-01 ir 2023-07-12 prašymus dėl JADIS / JARIS ir NTR naudotojų sąrašų atnaujinimo, prašė į duomenų

naudotojų sąrašus įtraukti juose nurodytus darbuotojus ir šiuose prašymuose nebuvo nurodyti statiniai (fiksiuoti) viešieji IP adresai, iš kurių jungsis prašymuose nurodyti darbuotojai. Atsižvelgdamas į tai, Registrų centras vertino, kad Migracijos departamentas, nenurodydamas išorinių IP adresų, išreiškė pageidavimą, kad prašymuose nurodytiems naudotojams duomenų teikimo sistema būtų leista naudotis kreipiantis iš bet kurio IP adreso ir į Migracijos departamentą su prašymu nurodyti išorinius IP adresus, iš kurių nurodyti naudotojai galės prisijungti prie NTR, nesikreipė.

Nors JAR 2017 sutarties 2020-04-20 Susitarimo 16 priedo 6.2 papunktyje nurodyta, kad jei išorinis IP adresas nėra nurodytas, paslaugų gavėjui yra leidžiama naudotis duomenų teikimo sistema, kreipiantis iš bet kurio IP adreso (t. y. ir iš užsienio), ši sutarties nuostata savaime nepatvirtina, kad toks prieigos suteikimo būdas atitinka BDAR reikalavimus. JAR 2017 sutarties 2020-04-20 Susitarime nustatyta prieigos suteikimo tvarka negali panaikinti ar sumažinti Registrų centrui pagal BDAR 5 straipsnio 1 dalies f punktą ir 32 straipsnį tenkančios savarankiškos pareigos įvertinti su pasirinktu prieigos modeliu susijusią riziką ir įgyvendinti pavojų atitinkančias technines bei organizacines saugumo priemones. Registrų centras, kaip duomenų tvarkytojas, administravo prieigas prie NTR ir JAR, taikydamas technines ir organizacines priemones, užtikrinančias asmens duomenų saugumą, todėl būtent jis turėjo techninę galimybę nustatyti, iš kokių IP adresų naudotojams leidžiama jungtis, atmesti prisijungimus iš nepatvirtintų IP adresų arba taikyti kitas papildomas prieigos kontrolės priemones. Migracijos departamentui prašymuose nenurodžius išorinių IP adresų, Registrų centras suteikė prieigą iš bet kurio IP adreso, tačiau kartu netaikė MFA ar kitos priemonės, kuri būtų kompensavusi dėl IP apribojimo netaikymo padidėjusią neteisėtos prieigos riziką. Taigi naudotojo tapatybei patvirtinti pakako vien naudotojo vardo ir slaptažodžio, o šiuos duomenis gavęs trečiasis asmuo galėjo jungtis prie registrų nepriklausomai nuo jo buvimo vietos ir naudojamo tinklo. Papildomai pažymėtina, kad Migracijos departamento sprendimas nenurodyti IP adresų negalėjo pakeisti Registrų centrui tiesiogiai iš BDAR kylančios pareigos užtikrinti tinkamą jo administruojamų sistemų saugumo lygį. Gavęs prašymus, kuriuose IP adresai nebuvo nurodyti, Registrų centras turėjo pareikalauti juos patikslinti arba taikyti kitas tinkamas prieigos kontrolės priemones, o ne automatiškai suteikti prieigą iš bet kurio IP adreso.

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad ADSP metu Registrų centro taikytas prieigos modelis, pagal kurį paveiktoms naudotojų paskyroms buvo leidžiama jungtis prie NTR ir JAR iš bet kurio IP adreso, tapatybę patvirtinant tik naudotojo vardu ir slaptažodžiu ir netaikant MFA ar kitų lygiaverčių papildomų prieigos kontrolės priemonių, neužtikrino pavojų atitinkančio saugumo lygio.

Papildomai pažymėtina, kad tyrimo metu nustatyta, jog tretiesiems asmenims pavyko prisijungti prie NTR ir JAR iš anksto žinant Migracijos departamento darbuotojų prisijungimo vardus ir slaptažodžius, tačiau jei jungiantis prie NTR ir JAR per išorinį tinklą (internetu) būtų taikomas MFA ar būtų įdiegtas prieigos ribojimas tik įgaliojams asmenims (pavyzdžiui, pagal iš anksto nurodytus IP adresus arba tik iš tam tikros teritorijos), piktavaliai nebūtų neteisėtai prisijungę prie NTR ir JAR.

ISO standarto 5.18 papunktyje „Prieigos teisės“ nustatyta, kad prieigos teisės turi būti suteikiamos, peržiūrimos, keičiamos ir panaikinamos pagal organizacijos prieigos valdymo taisykles, o prieigos teisės turi būti reguliariai peržiūrimos ir valdomos atsižvelgiant į informacijos saugumo reikalavimus, o 8.3 papunktyje „Prieigos prie informacijos ribojimas“ – kad prieiga prie informacijos ir kito susijusio turto turi būti ribojama taip, kad būtų užtikrinama tik leistina prieiga ir užkertamas kelias neleistinai prieigai. Šiame papunktyje taip pat nurodoma, kad turi būti taikomos loginės prieigos kontrolės priemonės, o prieigos leidimai gali būti ribojami atsižvelgiant į naudotojo tapatybę, vietą, naudojamą įrenginį ar kitus rizikos veiksnius.

Atsižvelgiant į tai, duomenų valdytojas ir duomenų tvarkytojas privalo užtikrinti, kad taikomos prieigos valdymo ir prieigos ribojimo priemonės būtų pakankamos užkirsti kelią neteisėtai

prieigai prie registruose tvarkomų asmens duomenų. Taikomos priemonės turi ne tik riboti galimybę naudotis esamais prisijungimo duomenimis, bet ir užtikrinti, kad tretieji asmenys negalėtų atkurti prieigos prie naudotojų paskyrų kitais būdais.

Tyrimo metu nustatyta, kad Migracijos departamento darbuotojai [DUOMENYS NESKELBTINI] dvi paskyros, skirtos prisijungti prie NTR ir JAR, buvo sukurtos nuo 2023-07-13, tačiau iki įvykstant ADSP darbuotoja nė karto nesijungė prie šių paskyrų. Darbuotojai [DUOMENYS NESKELBTINI] dvi paskyros buvo sukurtos nuo 2021-02-02 ir laikotarpiu nuo 2025-01-01 iki 2025-12-31 [DUOMENYS NESKELBTINI] nė karto nesijungė prie paskyrų. Taip pat tyrimo metu Migracijos departamentas pateikė [DUOMENYS NESKELBTINI] paaiškinimą dėl jungimosi prie paskyrų, kuriame buvo nurodyta, kad darbuotoja paskutinį kartą prie NTR paskyros galėjo jungtis 2024 m. liepos–rugsėjo mėn. Atsižvelgiant į tai nustatyta, kad viena Migracijos departamento darbuotoja jai suteiktomis naudotojo paskyromis nesinaudojo daugiau kaip 12 mėnesių, o kita darbuotoja suteiktomis naudotojo paskyromis nebuvo pasinaudojusi nė karto.

Registų centras atsakyme nurodė, kad neaktyvių naudotojų prieigų sustabdymui ADSP metu buvo taikomas naudotojo slaptažodžio galiojimo terminas (trys mėnesiai), kuriam pasibaigus prieiga prie duomenų tapdavo nebegalima. Prieigą buvo galima atkurti tik pasikeitus slaptažodį, pasinaudojant funkcija „Pamiršau slaptažodį“, kur be kitų duomenų turi būti nurodomas tikslus ir unikalus naudotojo vardas, o slaptažodžio keitimo nuoroda būdavo išsiunčiama į konkrečią naudotojo pašto dėžutę, kuri nurodyta vartotojų administravimo įrankyje [DUOMENYS NESKELBTINI]. Taip pat Registų centras nurodė, kad paveiktų paskyrų slaptažodžių galiojimas buvo pasibaigęs.

Inspekcija pažymi, kad neaktyvių naudotojų prieigos ribojimas, taikant slaptažodžio galiojimo terminą, nagrinėjamu atveju neužtikrino, jog pasibaigus slaptažodžio galiojimo terminui prieiga prie naudotojo paskyros negalėtų būti pakartotinai aktyvuota, kadangi ADSP metu tretieji asmenys, neteisėtai prisijungę prie Migracijos departamento darbuotojų el. pašto paskyrų, pasinaudojo slaptažodžio keitimo funkcionalumu, pakeitė NTR ir JAR naudotojų paskyrų slaptažodžius ir tokiu būdu įgijo prieigą prie NTR ir JAR, kuri vėliau buvo panaudota neteisėtam registruose tvarkomų asmens duomenų gavimui.

Atsižvelgiant į tai, darytina išvada, kad vien slaptažodžių galiojimo termino kontrolė nagrinėjamu atveju nebuvo pakankama prieigos valdymo ir prieigos ribojimo priemonė. Faktas, kad tretiesiems asmenims pavyko pakeisti nebegaliojančius slaptažodžius ir atkurti prieigą prie naudotojų paskyrų, patvirtina, jog taikytos priemonės neužtikrino pakankamos registruose tvarkomų asmens duomenų apsaugos nuo neteisėtos prieigos.

ISO standarto 8.16 papunktyje „Stebėsenos veikla“ nustatyta, kad organizacija turi nustatyti naudotojų įprastą veiklą ar elgseną (prieigos laiką, prieigos vietą, prieigos dažnumą ar kt.) ir pagal tai stebėti, ar nėra anomalijų.

VDAI gairių 122 punkte nustatyta, kad organizacija turi nusistatyti įprastą resursų naudojimą / našumą ir pagal jį stebėti, ar nėra neatitikimų.

Atsižvelgiant į nurodytas ISO standarto ir VDAI gairių nuostatas turi būti stebima kiekvieno naudotojo veikla ar elgsena.

Tyrimo metu nustatyta, kad Registų centras, 2026-04-01 gavęs Migracijos departamento prašymą dėl patikrinimo atlikimo ir įvertinęs žurnalinius įrašus, nustatė, jog laikotarpiu nuo 2026-01-06 iki 2026-04-01 buvo užfiksuotas itin didelis duomenų paieškos ir gavimo mastas (936 tūkst. veiksmų). Iki incidento atliekamų užklausų kiekiai buvo stebimi ir analizuojami duomenų gavėjo, bet ne konkretaus jo naudotojo, lygmeniu (šiuo atveju duomenų gavėjas buvo Vidaus reikalų ministerija, kurios užklausų kiekis dėl duomenų gavimo iš registų ir informacinių sistemų kitų duomenų gavėjų bendrame užklausų kontekste nebuvo neįprastai didelis).

Atsižvelgiant į tai, darytina išvada, kad Registrų centras neužtikrino pakankamos naudotojų veiklos stebėsenos ir anomalijų nustatymo priemonių, kadangi užklausų aktyvumas buvo vertinamas tik duomenų gavėjo, bet ne konkretaus naudotojo lygmeniu. Dėl šios priežasties nebuvo laiku identifikuota neįprasta veikla iš paveiktų paskyrų ir imtasi veiksmų galimam ADSP nustatyti bei jo pasekmėms sumažinti.

Pažymėtina, kad jei Registrų centras iki įvykstant ADSP būtų vertinęs atliekamų užklausų kiekį ne tik duomenų gavėjo (Vidaus reikalų ministerijos), bet ir kiekvieno naudotojo lygmeniu, būtų pastebėjęs, kad iš paveiktų paskyrų yra atliekamas neįprastai didelis užklausų skaičius ir ėmęsis veiksmų nustatyti, ar tokia neįprasta veikla yra teisėta, ar įvyko ADSP. Taip pat Registrų centras būtų galėjęs anksčiau sustabdyti trečiųjų šalių neteisėtus veiksmus, taip sumažinant paveiktų duomenų subjektų skaičių.

Apibendrinant dalyje „Dėl techninių ir organizacinių priemonių taikymo“ tyrimo metu nustatytą informaciją konstatuotina, kad ADSP mastui turėjo įtakos Registrų centro nepakankamai užtikrinama prieigų kontrolė ir autentifikavimas, kai naudotojams, jungiantis prie NTR ir JAR, nebuvo taikomas MFA, o IP filtravimo galimybė buvo palikta kaip pasirenkamoji ir paveiktų Migracijos departamento darbuotojų paskyrų atveju nebuvo taikoma. Registrų centras neužtikrino pakankamų prieigos valdymo ir ribojimo priemonių taikymo, kadangi taikyta nebegaliojančių slaptažodžių kontrolė buvo nepakankama ir neužkirto kelio tretiesiems asmenims atkurti prieigą prie NTR ir JAR naudotojų paskyrų, taip pat nepakankamai užtikrino kiekvieno naudotojo atliekamų užklausų stebėseną, kadangi atliekamų užklausų kiekiai buvo stebimi ir analizuojami tik duomenų gavėjo (Vidaus reikalų ministerijos), bet ne konkretaus jo naudotojo lygmeniu.

Remiantis tuo, kas nurodyta, darytina išvada, jog Registrų centras savo veiksmais (neveikimu) netinkamai įgyvendino ISO standarto 5.18, 8.3, 8.5 ir 8.16 papunkčių reikalavimus ir tokiu būdu pažeidė BDAR 5 straipsnio 1 dalies f punkte įtvirtintą konfidencialumo principą ir BDAR 32 straipsnio 1 dalies b punktą.

Įvykus ADSP Registrų centras [DUOMENYS NESKELBTINI].

Atsižvelgiant į tai, kas nurodyta, darytina išvada, kad įvykus ADSP Registrų centras ėmėsi reikiamų veiksmų, skirtų pašalinti priežastis, turėjusias įtakos ADSP kilimui.

Dėl pranešimo Inspekcijai ir duomenų subjektams apie ADSP

NTR nuostatų 11.5 papunktyje nustatyta, kad duomenų tvarkytojas privalo padėti duomenų valdytojui vykdant pareigas, nustatytas BDAR 33–34 straipsniuose, tai yra duomenų valdytojo nustatyta tvarka ir atvejais teikti pranešimus apie ADSP duomenų valdytojui, Inspekcijai ir duomenų subjektui, taip pat atlikti kitas reikalingas ADSP valdymo procedūras.

ADSP valdymo aprašo 2 punkte nustatyta, kad duomenų tvarkytojai Teisingumo ministerijos vardu atlieka asmens duomenų, tvarkomų Teisingumo ministerijos valdomuose registruose ir valstybės informacinėse sistemose, ADSP tyrimą bei kitas reikalingas ADSP valdymo procedūras, teikia pranešimus apie ADSP Inspekcijai ir duomenų subjektams šio aprašo nustatyta tvarka.

ADSP valdymo aprašo 10 punkte nustatyta, kad ADSP, kuris gali sukelti pavojų duomenų subjektų teisėms ir laisvėms, atveju duomenų tvarkytojas ne vėliau kaip per 72 valandas nuo tada, kai sužinojo apie ADSP, <...> pateikia pranešimą apie ADSP Inspekcijai ir Teisingumo ministerijai, o 14 punkte – kad kai dėl ADSP gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, duomenų tvarkytojas privalo nedelsdamas pranešti apie ADSP tiesiogiai duomenų subjektui, Inspekcijai ir Teisingumo ministerijai.

Atsižvelgiant į nurodytas teisės aktų nuostatas darytina išvada, kad už tinkamą pareigų, numatytų BDAR 33 ir 34 straipsniuose, vykdymą yra atsakingas Registrų centras.

BDAR 33 straipsnio 1 dalyje nustatyta, kad ADSP atveju duomenų valdytojas nepagrįstai nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo tada, kai jis sužino apie ADSP, apie tai praneša priežiūros institucijai, nebent ADSP neturėtų kelti pavojaus fizinių asmenų teisėms ir laisvėms, o 34 straipsnio 1 dalyje – kad kai dėl ADSP gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nepagrįstai nedelsdamas praneša apie ADSP duomenų subjektui.

Nagrinėjamu atveju, atsižvelgiant į BDAR preambulės 75 punktą, ADSP metu paveiktų asmens duomenų pobūdį (vardai, pavardės, asmens kodai, informacija apie nekilnojamąjį turtą ir kt.) ir didelį kiekį paveiktų asmens duomenų ir duomenų subjektų, įvykęs ADSP neabejotinai gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms, taigi duomenų tvarkytojas (Registrų centras) apie įvykusį ADSP turėjo pranešti Inspekcijai per 72 valandas nuo tada, kai apie jį sužinojo, taip pat turėjo nepagrįstai nedelsdamas informuoti duomenų subjektus.

Iš tyrimo medžiagos matyti, kad Registrų centras 2026-04-13 informavo Inspekciją, jog 2026-04-01 Migracijos departamentas pranešė apie galimai prarastus prisijungimo prie NTR duomenis ir galimą jų panaudojimą gaunant NTR duomenis, pažymėjo, jog detalesnės įvykio aplinkybės pateiktos nebuvo, tačiau, nepaisant to, reaguodamas į situaciją, ėmėsi prevencinių veiksmų, inicijavo kreipimąsi į Lietuvos kriminalinės policijos biurą dėl įvykio įvertinimo ir tyrimo atlikimo, užregistravo galimai įvykusį kibernetinį incidentą Nacionalinėje incidentų valdymo sistemoje NKSC, įvykio aplinkybių patikrinimas yra atliekamas Informatikos ir ryšių departamente bei Migracijos departamente. Registrų centras pažymėjo, kad inicijuoti tyrimai ir patikrinimai nėra baigti, tik juos pabaigus bus galima objektyviai ir patikimai spręsti apie nurodyto įvykio kilmę, pobūdį, poveikį tvarkomiems duomenims ir apie tai Inspekcija bus informuota atskirai.

Po to, 2026-05-07, Registrų centras pateikė pranešimą apie ADSP, kuriame pažymėjo, jog ADSP nustatymo data – 2026-05-07, taip pat nurodė duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičių, kategorijas ir kt., pažymėjo, jog vis dar nėra gavęs oficialiai patvirtintos informacijos apie tai, ar duomenų gavėjo pusėje yra įvykęs ADSP, bet, nepaisant to, įtariant piktaivališkus veiksmus NTR duomenų gavimo užklausoje, taip pat įtarimus keliančių naudotojų atliktas paieškas ir peržiūras JAR, 2026-05-07 nuspręsta atvejį laikyti ADSP. Taip pat pažymėjo, kad duomenų subjektai apie įvykusį ADSP nėra informuoti, nes 2026-05-07 kreiptasi į ikiteisminio tyrimo instituciją prašant pateikti informaciją apie sprendimą dėl ikiteisminio tyrimo medžiagoje esančių incidento duomenų viešinimo BDAR nustatyta tvarka.

Registrų centras 2026-05-28 rašte Inspekcijai nurodė, kad 2026-05-07, kreipiantis į Generalinę prokuratūrą, buvo prašoma pateikti informaciją apie sprendimą dėl ikiteisminio tyrimo medžiagoje esančių incidento duomenų viešinimo BDAR nustatyta tvarka ir 2026-05-14 gautas atsakymas, jog BDAR 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija ir priemonės neturi ikiteisminio tyrimo duomenų požymių ir šiai informacijai netaikoma ikiteisminio tyrimo duomenų apsauga bei darytina išvada, kad duomenų valdytojas turėtų vykdyti BDAR 34 straipsnyje nustatytą įpareigojimą, nesikreipdamas dėl leidimo gavimo į ikiteisminį tyrimą organizuojantį prokurorą. Registrų centras pažymėjo, jog paraleliai pateiktam užklausaui Generalinei prokuratūrai vyko aktyvus pasirengimas atvejui, jeigu duomenų subjektų informavimas apie ADSP bus suderinamas su ikiteisminio tyrimo vykdymu, t. y. rengiamas specialus techninis sprendimas Registrų centro savitarnos sistemoje, kuriuo naudodamiesi asmenys, tinkamai save identifikavę, galėtų patys pasitikrinti, ar jų asmens duomenys, esantys Nekilnojamojo turto registre, buvo atskleisti, taip pat gauti BDAR 34 straipsnyje numatytą informaciją. Nuo 2026-05-25, baigus techninio sprendimo įgyvendinimo darbus, šis sprendimas tapo pasiekiamas visiems duomenų subjektams, kurie jungiasi prie Registrų centro savitarnos. Taip pat informacija, ar konkretaus asmens duomenys, esantys Nekilnojamojo turto registre, buvo atskleisti, teikiama visuose Registrų centro klientų aptarnavimo padaliniuose. Be to, duomenų subjektams apie ADSP pranešta ir viešais

pranešimais Registrų centro svetainėje, Facebook paskyroje, naujienų portaluose. Papildomai nurodė, kad specialus techninis sprendimas Registrų centro savitarnos sistemoje neapima duomenų subjektų, kurių asmens duomenys buvo atskleisti suformavus Juridinių asmenų registro išrašus ir atsižvelgiant į tai, kad buvo nutekinti 30 juridinių asmenų išplėstiniai išrašai ir 3 juridinių asmenų išplėstiniai išrašai su istorija, o nutekintuose išrašuose yra nurodytas kontaktinis duomenų subjektų adresas, šie asmens informuojami individualiai, pranešimus apie ADSP išsiunčiant paštu.

Europos duomenų apsaugos valdybos 2023-03-28 gairėse Nr. 9/2022 dėl pranešimo apie asmens duomenų saugumo pažeidimus pagal BDAR (toliau – Gairės dėl ADSP) nurodyta, kad duomenų valdytojas turėtų būti laikomas žinančiu apie pažeidimą, kai jis pakankamai įsitikina, kad įvyko saugumo incidentas, dėl kurio kilo pavojus asmens duomenų saugumui. Taip pat pažymėta, jog duomenų valdytojas, asmens, žiniasklaidos organizacijos ar kito šaltinio informuotas apie galimą pažeidimą arba pats nustatęs saugumo incidentą, gali atlikti trumpą tyrimą, kad nustatytų, ar pažeidimas iš tikrųjų buvo padarytas. Šio tyrimo laikotarpiu duomenų valdytojas negali būti laikomas žinančiu apie pažeidimą. Tačiau tikimasi, kad kuo skubiau bus pradėtas pirminis tyrimas ir pakankamai patikimai nustatyta, ar buvo padarytas pažeidimas; tada gali būti atliekamas išsamesnis tyrimas.

Išnagrinėjus tyrimo medžiagoje esančią informaciją nustatyta, kad Registrų centras Inspekcijai pranešimą apie ADSP pateikė 2026-05-07. Taip pat nustatyta, jog Migracijos departamentas apie galimai prarastus NTR duomenis ir tai, kad NTR duomenys, naudojantis Migracijos departamento darbuotojos paskyra, buvo tikrinami iš IP adreso Malaizijoje, Registrų centrą informavo 2026-04-01. Registrų centras 2026-04-08 rašte Migracijos departamentui nurodė, jog patikrinęs naudotojo [DUOMENYS NESKELBTINI] veiksmų analizę pastebėjo didelius duomenų paieškos ir gavimo iš registro kiekius, taip pat atlikus kitų Migracijos departamento naudotojų veiksmų registre analizę nustatyti dideli naudotojo [DUOMENYS NESKELBTINI] duomenų paieškų ir gavimo iš registro kiekiai tuo pačiu laikotarpiu. Registrų centras Migracijos departamentui šiame rašte nurodė gana tikslų veiksmų (įrašų formavimo, daiktų paieškos pagal adresą ir kt.) skaičių, taip pat jog nustatė, kad 2026-01-06 ir 2026-01-20 buvo fiksuoti slaptažodžių keitimai, bei ėmėsi prevencinių veiksmų (užblokavo naudotojus, apie incidentą informavo NKSC, užblokavo IP adresus).

Inspekcija, įvertinusi nurodytą informaciją bei Registrų centro atliktus veiksmus, vertina, kad Registrų centras 2026-04-08 (teikdamas informaciją Migracijos departamentui) neabejotinai žinojo apie įvykusį ADSP, tačiau pranešimą apie ADSP Inspekcijai pateikė tik 2026-05-07. Pažymėtina, jog Registrų centrui, nustačius itin didelės apimties duomenų užklausas naudojantis dviem paskyromis, taip pat turint informaciją, kad duomenys buvo tvarkomi (tikrinami) iš IP adresų Malaizijoje, neturėjo kilti abejonių, jog nagrinėjamu atveju įvyko ADSP. Juo labiau, Migracijos departamentas Registrų centrui nurodė, kad darbuotojos [DUOMENYS NESKELBTINI] prisijungimo duomenys galimai buvo gauti neteisėtu būdu ir iš registrų duomenys buvo paimti neteisėtu būdu. Pažymėtina, kad pats Registrų centras, gavęs Migracijos departamento pranešimą dėl įvykusio incidento, iš karto ėmėsi prevencinių veiksmų, kreipėsi į NKSC bei Generalinę prokuratūrą, kas rodo, kad jau buvo pakankamai patikimai nustatyta, jog įvyko incidentas, kurio metu buvo paveikti asmens duomenys. Atsižvelgiant į nurodytas aplinkybes, Registrų centro teiginiai, kad 2026-05-07, teikdamas pranešimą apie ADSP, jis neturėjo oficialiai patvirtintos informacijos apie tai, kad įvyko ADSP, vertintini kritiškai.

Remiantis tuo, kas aukščiau nurodyta, Inspekcija sprendžia, kad Registrų centras, turėdamas pareigą per 72 valandas nuo tada, kai sužinojo apie įvykusį ADSP, apie tai informuoti Inspekciją, to nepadarė.

Iš tyrimo medžiagoje esančio Generalinės prokuratūros rašto matyti, kad Registrų centras 2026-05-14 buvo informuotas, jog BDAR 33 straipsnio 3 dalies b, c ir d punktuose nurodytai informacijai (kuri pagal BDAR 34 straipsnio 2 dalį turi būti pateikta duomenų subjektui) netaikoma ikiteisminio tyrimo duomenų apsauga. Registrų centras apie įvykusį ADSP 2026-05-22 paskelbė viešais pranešimais Registrų centro svetainėje, Facebook paskyroje, naujienų portaluose (www.lrt.lt),

www.delfi.lt), taip pat nuo 2026-05-25 įgyvendino techninį sprendimą Registrų centro savitarnos sistemoje, kuriuo naudodamiesi asmenys, tinkamai save identifikavę, galėjo patys patikrinti, ar jų asmens duomenys, esantys NTR, buvo atskleisti, taip pat gauti BDAR 34 straipsnyje numatytą informaciją, o nuo 2026-05-26 informaciją apie atskleistus JAR duomenis duomenų subjektams pateikė el. paštu.

Gairėse dėl ADSP nurodyta, kad remiantis BDAR, asmenims apie ADSP turėtų būti pranešama „nepagrįstai nedelsiant“, t. y. kuo skubiau. Pagrindinis pranešimo asmenims tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jie turėtų imtis, kad apsaugotų. Atsižvelgiant į ADSP pobūdį ir keliamą pavojų, laiku pateikus pranešimą, asmenims bus lengviau imtis veiksmų norint apsaugoti nuo galimų neigiamų pažeidimo pasekmių.

Inspekcija, įvertinusi tyrimo metu nustatytą informaciją, sprendžia, kad, atsižvelgiant į itin didelį duomenų subjektų, kurių asmens duomenų saugumas buvo pažeistas, skaičių, Registrų centras pasirinko tinkamą būdą (viešą paskelbimą ir informacijos pateikimą Registrų centro savitarnos svetainėje asmenims, kurių duomenys buvo tvarkomi NTR, bei el. paštu asmenims, kurių duomenys buvo tvarkomi JAR) pranešti apie įvykusį ADSP, tačiau, pažymėtina, kad įvertinus aplinkybę, jog Generalinė prokuratūra 2026-05-14 informavo, kad informacijai, kuri pagal BDAR 34 straipsnio 2 dalį turi būti pateikta duomenų subjektui, netaikoma ikiteisminio tyrimo duomenų apsauga, spręstina, kad duomenų subjektai apie įvykusį ADSP nebuvo informuoti nepagrįstai nedelsiant. Pažymėtina, kad Registrų centras į Generalinę prokuratūrą dėl informacijos, ar gali būti atskleista (paviešinta) BDAR 33 straipsnio 3 dalies b, c ir d punktuose nurodyta informacija, kreipėsi 2026-05-07. Taigi jau išsiuntęs šį paklausimą Generalinei prokuratūrai, kaip duomenų tvarkytojas, atsakingas už pranešimo apie įvykusį ADSP pateikimą duomenų subjektams, ypač žinodamas ADSP mastą, paveiktų asmenų skaičių, Registrų centras turėjo pasirengti iš anksto ir gavęs atsakymą, jog ši informacija gali būti atskleista (paviešinta), duomenų subjektus apie įvykusį ADSP bent jau viešo paskelbimo būdu turėjo informuoti iš karto, o ne praėjus daugiau nei savaitei po to, kai gavo Generalinės prokuratūros atsakymą.

Remiantis tuo, kas aukščiau nurodyta, Inspekcija sprendžia, kad Registrų centras, turėdamas pareigą apie įvykusį ADSP nepagrįstai nedelsiant informuoti duomenų subjektus, to nepadarė.

Apibendrinant šio sprendimo dalyje „Dėl pranešimo Inspekcijai ir duomenų subjektams apie ADSP“ tyrimo metu nustatytą informaciją konstatuotina, kad Registrų centras, turėdamas pareigą per 72 valandas nuo tada, kai sužinojo apie įvykusį ADSP, apie tai informuoti Inspekciją ir nepagrįstai nedelsiant informuoti duomenų subjektus, to nepadarė.

Remiantis tuo, kas nurodyta, darytina išvada, jog Registrų centras savo veiksmais (neveikimu) pažeidė BDAR 33 straipsnio 1 dalies ir 34 straipsnio 1 dalies nuostatas.

Dėl poveikio priemonių

BDAR preambulės 129 punkte numatyta, jog kiekviena priežiūros institucijos taikoma priemonė turi būti tinkama, būtina ir proporcinga siekiant užtikrinti šio reglamento laikymąsi, atsižvelgiant į kiekvieno konkretaus atvejo aplinkybes.

Sprendžiant dėl poveikio priemonių skyrimo Informatikos ir ryšių departamentui Inspekcija atsižvelgia į tai, kad Informatikos ir ryšių departamentas neįgyvendino techninių ir organizacinių saugumo priemonių, kad užtikrintų prieigų kontrolę ir autentifikavimo priemonių taikymą, tinkamai neįvertino įvykusio saugumo incidento, dėl ko tretieji asmenys gavo neteisėtą prieigą prie Migracijos departamento el. pašto paskyrų ir, jomis pasinaudoję, atkūrė prisijungimo prie NTR ir JAR slaptažodžius neteisėtai prieigai prie daugiau kaip 500 000 duomenų subjektų asmens duomenų, taip pat į tai, kad apie saugumo spragas ir nepakankamą techninių ir organizacinių priemonių

taikymą / netaikymą žinojo iki įvykstant ADSP, tačiau saugumo spragų nepašalino ir tinkamų techninių ir organizacinių priemonių laiku bei tinkamai neįgyvendino, ir nusprendžia už BDAR 5 straipsnio 1 dalies f punkto, 32 straipsnio 1 dalies b punkto pažeidimus pradėti Informatikos ir ryšių departamento atžvilgiu administracinės baudos skyrimo procedūrą. Atsižvelgiant į tai, kad įvykus ADSP Informatikos ir ryšių departamentas ėmėsi reikiamų veiksmų, teikti nurodymą suderinti duomenų tvarkymo operacijas su BDAR nuostatomis nėra pagrindo.

Sprendžiant dėl poveikio priemonių skyrimo Migracijos departamentui Inspekcija atsižvelgia į tai, kad Migracijos departamentas, teikdamas prašymus Registrų centrui dėl naudotojų įtraukimo į NTR ir JAR duomenų naudotojų sąrašus nenurodė konkrečių išorinių IP adresų, nesiėmė visų priemonių, kurios galėjo sumažinti neteisėtos prieigos prie NTR ir JAR riziką, taip pat į tai, kad tokie veiksmai (neveikimas) savaime nesukūrė galimybės tretiesiems asmenims gauti prieigą prie asmens duomenų ir neturėjo esminės įtakos įvykusiam ADSP, ir sprendžia, kad nagrinėjamu atveju Migracijos departamentui už BDAR 24 straipsnio 1 dalies pažeidimą, vadovaujantis BDAR 58 straipsnio 2 dalies b punktu, pareiškiamas papeikimas. Atsižvelgiant į tai, kad įvykus ADSP Migracijos departamentas ėmėsi reikiamų veiksmų, teikti nurodymą suderinti duomenų tvarkymo operacijas su BDAR nuostatomis nėra pagrindo. Kitų poveikio priemonių taikymas nagrinėjamu atveju nebūtų proporcingas.

Sprendžiant dėl poveikio priemonių skyrimo Registrų centrui Inspekcija atsižvelgia į tai, kad Registrų centras neįgyvendino techninių ir organizacinių saugumo priemonių, kad užtikrintų prieigų kontrolę ir autentifikavimą, kiekvieno naudotojo atliekamų užklausų stebėseną, dėl ko tretieji asmenys gavo prieigą prie NTR bei JAR duomenų ir dėl to buvo paveikti daugiau nei 500 000 duomenų subjektų asmens duomenys, taip pat laiku neinformavo Inspekcijos ir duomenų subjektų apie įvykusį ADSP ir nusprendžia už BDAR 5 straipsnio 1 dalies f punkto, 32 straipsnio 1 dalies b punkto, 33 straipsnio 1 dalies, 34 straipsnio 1 dalies pažeidimus pradėti Registrų centro atžvilgiu administracinės baudos skyrimo procedūrą. Atsižvelgiant į tai, kad įvykus ADSP Registrų centras ėmėsi reikiamų veiksmų, teikti nurodymą suderinti duomenų tvarkymo operacijas su BDAR nuostatomis nėra pagrindo.

Inspekcija, vadovaudamasi Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 22 straipsnio 1 dalies 2 punktu, BDAR 58 straipsnio 2 dalies b ir i punktais,

n u s p r e n d ž i a:

1. Informatikos ir ryšių departamento atžvilgiu už BDAR 5 straipsnio 1 dalies f punkte įtvirtinto konfidencialumo principo ir 32 straipsnio 1 dalies b punkto pažeidimus pradėti administracinės baudos skyrimo procedūrą.
2. Migracijos departamentui už BDAR 24 straipsnio 1 dalies pažeidimą pareikšti papeikimą.
3. Registrų centro atžvilgiu už BDAR 5 straipsnio 1 dalies f punkte įtvirtinto konfidencialumo principo, 32 straipsnio 1 dalies b punkto, 33 straipsnio 1 dalies ir 34 straipsnio 1 dalies pažeidimus pradėti administracinės baudos skyrimo procedūrą.

Šis sprendimas Administracinių bylų teisenos įstatymo nustatyta tvarka per vieną mėnesį nuo jo įteikimo dienos gali būti skundžiamas Regionų administraciniam teismui (adresas: Žygimantų g. 2, Vilnius).

Direktorė

Dijana Šinkūnienė