LVK Lietuvos verslo konfederacija

+370 5 212 1111 Gedimino pr. 2/1-28 lvk.lt
info@lvk.lt LT-01103 Vilnius

Lietuvos Respublikos Vyriausybei
Sveikatos apsaugos ministerijai
Ekonomikos ir inovacijų ministerijai
Krašto apsaugos ministerijai
Nacionaliniam kibernetiniam saugumo centrui

2026 m. gegužės 29 d., Nr. 26-089AR

Kopija:
Lietuvos Respublikos Seimo Sveikatos reikalų komitetui

DĖL SVEIKATOS DUOMENŲ TVARKYMO IR KIBERNETINIO SAUGUMO VALSTYBĖS INFORMACINĖSE SISTEMOSE

Naujausias incidentas VĮ „Registrų centras" valdomose informacinėse sistemose, dėl kurio 2026 m. gegužės 22 d. Generalinė prokuratūra pradėjo ikiteisminį tyrimą, o Valstybinė duomenų apsaugos inspekcija – tyrimą dėl asmens duomenų saugumo pažeidimo, dar kartą atskleidė sisteminius valstybės skaitmeninės infrastruktūros atsparumo trūkumus.

Pagal viešai paskelbtą oficialią informaciją, neteisėti prisijungimai prie valstybės valdomų duomenų registrų buvo vykdomi iš užsienio valstybės, be kita ko, per kitų institucijų administruojamas sistemas. Įtariama, kad galėjo būti neteisėtai nukopijuota daugiau kaip 600 tūkst. registrų įrašų, o pagrindinis taikinys buvo Nekilnojamojo turto registro ir Juridinių asmenų registro duomenys.

Šis incidentas įgauna ypatingą reikšmę vertinamas kartu su dviem naujausiais reguliaciniais pokyčiais sveikatos duomenų tvarkymo srityje – Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) paskyrimu ESPB IS tvarkytoja ir savarankiškos VLIVAS IS įsteigimu. Jie kyla iš šių, jau priimtų teisės aktų:

1. Lietuvos Respublikos sveikatos apsaugos ministro 2026 m. kovo 25 d. įsakymu Nr. V-267 patvirtintais Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (toliau – ESPB IS) nuostatų pakeitimais, kuriais **VLK paskiriama papildoma ESPB IS tvarkytoja**; ir

2. VLK direktoriaus 2026 m. balandžio 29 d. įsakymu Nr. 1K-174 patvirtintais **naujos Vieningos ligoninių išteklių valdymo ir sąnaudų apskaitos informacinės sistemos** (toliau – VLIVAS IS) nuostatais (toliau – Nuostatai).

Šie teisės aktai kartu sudaro precedento neturintį teisinį pagrindą VLK tapti centrine dviejų ypatingai jautrių sveikatos duomenų informacinių sistemų figūra. Tuo pat metu, kai VĮ „Registrų centras" ištiko duomenų saugumo incidentas, nepaisant jam taikomų papildomų nacionalinio saugumo patikros reikalavimų, kurių laikymasis vis tiek neužkirto kelio incidentui įvykti.

Šiuo kreipimusi Lietuvos verslo konfederacija (toliau – LVK) siekia atkreipti kompetentingų valstybės sprendimų priėmėjų dėmesį į struktūrinę riziką, kylančią iš šių dviejų tendencijų derinio, ir pasiūlyti reguliacines bei institucines priemones sveikatos duomenų ir valstybės informacinių

+370 5 212 1111 Gedimino pr. 2/1-28 lvk.lt
info@lvk.lt LT-01103 Vilnius

sistemų apsaugai sustiprinti. LVK vertinimu, šios priemonės yra būtinos ypatingos svarbos valstybės sektoriaus – sveikatos sektoriaus – skaitmeninio atsparumo užtikrinimui.

I. Naujai kuriamos ir plečiamos nacionalinio lygmens sveikatos duomenų tvarkymo sistemos

I.1. ESPB IS nuostatų pakeitimai – VLK kaip papildoma „e.sveikata" tvarkytoja

Lietuvos Respublikos sveikatos apsaugos ministro 2026 m. kovo 25 d. įsakymu Nr. V-267 patvirtinti ESPB IS nuostatų pakeitimai įtvirtina iš esmės naują teisinę situaciją. VLK paskiriama ESPB IS tvarkytoja šalia jau esamų tvarkytojų (įskaitant VĮ „Registrų centras"), tačiau jai pavedama ypatinga funkcija – organizuoti ESPB IS vystymą ir priežiūrą. Tai reiškia, kad VLK tampa neatsiejama esamos centrinės e.sveikata sistemos dalimi – sistemos, kurioje kaupiami itin jautrūs duomenys (elektroniniai sveikatos įrašai, receptai, gydymo istorija, laboratorinių tyrimų rezultatai) apie visus Lietuvos gyventojus.

Šie pakeitimai iš esmės keičia VLK vaidmenį – iš finansų ir sveikatos draudimo lėšų srities reguliatoriaus ji tampa informacinės sistemos, kurioje saugomi visų šalies gyventojų sveikatos duomenys, technine prižiūrėtoja ir vystytoja. Toks vaidmenų išplėtimas reikalauja atitinkamo institucinio pajėgumo, techninės kompetencijos ir, svarbiausia, adekvataus teisinio reguliavimo bei papildomų saugumo garantijų, be kita ko – pasitelkiamų tiekėjų ir kitų trečiųjų asmenų patikros procedūrų.

I.2. VLIVAS IS – *de facto* paralelinė e.sveikata sistema

Priėmus VLK direktoriaus 2026 m. balandžio 29 d. įsakymą Nr. 1K-174, VLIVAS IS tapo visuotine, visoms asmens sveikatos priežiūros įstaigoms (toliau – ASPĮ) be jokių išlygų ir alternatyvų privaloma naudoti informacine sistema.

Susiejus VLIVAS IS funkcijas su Nuostatų 16 punkte nurodytomis tvarkomų asmens duomenų kategorijomis – sąrašą sudaro 8 pagrindinės kategorijos, apimančios iš viso 92 rūšių duomenis – galima konstatuoti, kad VLIVAS IS numatomas ne vien agreguotų finansinių ar apskaitos duomenų tvarkymas, kaip deklaruojama Nuostatų 2 punkte. **Tokia duomenų apimtis rodo iš esmės kitokį duomenų tvarkymo modelį – VLIVAS IS faktiškai priartėja prie paralelinės pacientų sveikatos duomenų infrastruktūros, nors deklaruojamas tikslas yra sąnaudų apskaita ir sveikatos priežiūros paslaugų prieinamumo stebėsena**.

Konkrečiau, tokia informacinė sistema faktiškai sukuria ne tik itin plačios apimties duomenų bazę, kurioje galima rekonstruoti paciento apsilankymų, tyrimų, procedūrų, diagnozių, paslaugų ir jas teikusių darbuotojų tikslią chronologiją, bet ir sudaro sąlygas unikaliai individualizuoti bei profiliuoti duomenų subjektus – tiek pacientus, tiek ASPĮ darbuotojus – remiantis VLIVAS IS numatytais duomenų pjūviais.

VLIVAS IS tvarkomų duomenų apimtis ir duomenų modelio architektūra leidžia susieti (i) pacientą, (ii) ASPĮ, (iii) pacientams suteiktas paslaugas, (iv) pacientams atliktus tyrimus, procedūras, nustatytas diagnozes ar kitus sveikatos priežiūros paslaugų teikimo proceso duomenis, (v) ASPĮ patirtų sąnaudų elementus, (vi) konkrečius ASPĮ darbuotojus, (vii) šių darbuotojų pareigybių, specialybių, tabelio ir darbo užmokesčio bei sąnaudų grupių duomenis. Faktiškai sukuriama centralizuota sveikatos duomenų infrastruktūra, kuri iš esmės atitinka ESPB IS (e.sveikata) funkcinę apimtį.

Todėl abu šie pokyčiai – VLK paskyrimas ESPB IS tvarkytoja ir savarankiškos VLIVAS IS įsteigimas – sudaro sąlygas VLK tapti itin jautrių sveikatos duomenų ne tik tvarkytoja (ESPB IS atveju), bet ir valdytoja (VLIVAS IS atveju) be atitinkamų nacionalinio saugumo ir kibernetinio atsparumo garantijų.

II. Registrų centro incidento precedentas

II.1. Registrų centras kaip pirmos kategorijos nacionaliniam saugumui svarbi įmonė

VĮ „Registrų centras“ yra laikomas pirmos kategorijos nacionaliniam saugumui užtikrinti svarbia įmone pagal Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 1 priedo 7 dalį. Dėl šio statuso VĮ „Registrų centras“ taikomi itin griežti sandorių atitikties nacionalinio saugumo interesams patikros reikalavimai, be kita ko, Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos atliekama patikra dėl VĮ „Registrų centras“ pasitelktos sandorio šalies, kuriai planuojama suteikti prieigą prie nacionaliniam saugumui užtikrinti svarbių įrenginių ir turto, kuris kelia riziką ar grėsmę nacionaliniam saugumui (Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo 13 straipsnis).

Be to, VĮ „Registrų centras“ taikomi ir aukščiausi kibernetinio saugumo reikalavimai kaip esminiam kibernetinio saugumo subjektui pagal NIS2 direktyvą ir ją į nacionalinę teisę perkėlusį Lietuvos Respublikos kibernetinio saugumo įstatymą.

II.2. Papildomos saugumo priemonės neužkirto kelio incidentui

Nepaisant šio itin griežto reguliacinės ir saugumo kontrolės režimo – nacionalinio saugumo sandorių patikros reikalavimų ir aukščiausių kibernetinio saugumo standartų taikymo – didžiulis duomenų saugumo incidentas vis tiek įvyko. LVK nesiima vertinti šio incidento tikrųjų priežasčių, tačiau negali nekreipti dėmesio į paties VĮ „Registrų centras“ ankstesniųjų metų strateginiuose dokumentuose atskleidžiamas sistemines problemas valstybės skaitmeninės infrastruktūros valdyme:

- 60 proc. registrų informacinių sistemų naudojama programinė įranga yra senesnė nei 8 metų ir kelia architektūrinius bei kibernetinio saugumo iššūkius;
- finansavimas pavestoms valstybinėms funkcijoms vykdyti yra nepakankamas;
- veiklos tęstinumo srityje egzistuoja svarbios spragos – trūksta geografiškai nutolusių duomenų centrų, neužtikrinamas kritinių duomenų atkūrimas.

Taigi, griežčiausias galimas teisinio reguliavimo režimas – pirmos kategorijos nacionaliniam saugumui svarbios įmonės statusas, sandorių patikros reikalavimai ir esminiam kibernetinio saugumo subjektui taikomi standartai – neleido nei laiku identifikuoti, nei užkirsti kelio incidentui. Problemos šaknys yra kur kas gilesnės. LVK tai kelia esminį klausimą – kokius standartus turi atitikti dar jautresnių duomenų, pavyzdžiui, visų Lietuvos gyventojų sveikatos duomenų, valstybinių informacinių sistemų tvarkytojai.

II.3. Sveikatos duomenys – aukštesnio apsaugos lygio duomenų kategorija

Dar griežtesni duomenų tvarkymo reikalavimai galioja sveikatos duomenims – pagal BDAR 9 straipsnį jie priskiriami specialiųjų kategorijų asmens duomenims, kurių tvarkymui taikomi patys aukščiausi apsaugos standartai. Tai reiškia, kad bet koks sveikatos duomenų tvarkymas valstybinėse informacinėse sistemose reikalauja ne mažesnio, o dar griežtesnio saugumo ir priežiūros režimo nei tas, kuris nesugebėjo apsaugoti VĮ „Registrų centras“ tvarkomų duomenų.

+370 5 212 1111 Gedimino pr. 2/1-28 lvk.lt
info@lvk.lt LT-01103 Vilnius

III. VLK statuso problematika

III.1. Dviguba VLK funkcija

Kaip paaiškinta aukščiau, dėl ESPB IS nuostatų pakeitimo ir VLIVAS IS nuostatų priėmimo VLK tampa:

1. **ESPB IS (e.sveikata) tvarkytoja**, kuriai priskirta ypatingai svarbi šios informacinės sistemos vystymo ir techninės priežiūros funkcija – t. y. faktiškai pagrindinė nacionalinės e.sveikatos informacinės sistemos saugios jos veiklos užtikrinimo (informacijos konfidencialumas, vientisumas ir prieinamumas) ir tolesnio šios sistemos vystymo grandis;
2. **VLIVAS IS valdytoja**, vykdanti visapusišką savo pačios kuriamos informacinės sistemos apsaugą.

Tai reiškia, kad viena viešojo administravimo institucija tampa atsakinga už dviejų ypatingai jautrių nacionalinio masto sveikatos duomenų informacinių sistemų tvarkymą, nors net specializuota valstybės įmonė, įsteigta išimtinai tvarkyti valstybės informacinius išteklius ir turinti atitinkamus techninius, organizacinius ir žmogiškuosius resursus (techninės specializacijos personalą), nesugebėjo išvengti įvykusio incidento.

Tai kelia pagrįstų abejonių, ar valstybės šia linkme formuojama politika – svarbiausių valstybės informacinių sistemų tvarkymo išdalinimas viešojo administravimo institucijoms – yra teisinga. LVK vertinimu, toks skaidymas neišvengiamai sukurs nepageidaujamą efektą: reikiamos kompetencijos, kvalifikacijos ir dedikuoto personalo neturinčios viešojo administravimo institucijos tokias paslaugas paprasčiausiai turės pirkti iš išorės tiekėjų, o tai savo ruožtu užprogramuoja naują riziką – šių tiekėjų patikimumo ir jų veiklos tinkamos priežiūros klausimą.

III.2. Sandorių atitikties patikros reikalavimų nebuvimas

Esminė tokio sprendimo – paskirti viešojo administravimo instituciją valstybės informacinių sistemų, kuriose tvarkomi ypatingos svarbos ir svarbūs valstybės informaciniai ištekliai, tvarkytoja – problema yra ta, kad, priešingai nei VĮ „Registrų centras“, VLK šiuo metu **nėra taikomi** sandorių atitikties nacionalinio saugumo interesams patikros reikalavimai pagal Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymą. Tai reiškia, kad:

- VLK, tapusi ESPB IS tvarkytoja ir VLIVAS IS valdytoja, gali sudaryti sutartis su trečiosiomis šalimis, suteikdama joms prieigą prie ypatingai jautrių valstybės informacinių sistemų, be nacionalinio saugumo interesams atliktos trečiosios šalies patikros;
- nėra mechanizmo, kuris užtikrintų, kad asmenys ar organizacijos, gaunantys prieigą prie atitinkamų valstybės informacinių sistemų, nekeltų grėsmės nacionaliniam saugumui;
- VĮ „Registrų centras“ – tvarkantis asmens duomenų apsaugos prasme mažiau jautrius duomenis, nei numatoma tvarkyti VLIVAS IS ir jau tvarkoma ESPB IS – turi griežtesnį saugumo patikros režimą nei VLK.

Ši situacija yra paradoksali ir sukuria potencialiai didesnes grėsmes ypatingos svarbos ir svarbiems valstybės informaciniams ištekliams, kuriuos tvarkys ar jau tvarko viešojo administravimo subjektai, kadangi rizikos veiksnių skaičius ne mažinamas, o atvirkščiai – didinamas, be jokio kompensacinio mechanizmo – bent jau griežtesnių sandorių patikros reikalavimų pavidalu. Be to, dėl ESPB IS nuostatų pakeitimo susidaro situacija, kai tos pačios informacinės sistemos (ESPB IS) tvarkytojo funkcijos pasidalija tarp dviejų institucijų – VĮ „Registrų centras“ ir VLK, kurioms taikomi iš esmės

skirtingi saugumo patikros režimai. Toks nevienalytis saugumo reikalavimų taikymas tos pačios valstybės informacinės sistemos tvarkytojams ne tik nesumažina, bet dar labiau padidina sisteminę riziką, nes bendras sistemos saugumo lygis neišvengiamai nulemtas silpniausios grandies.

LVK vertinimu, ne svarbiausių valstybės informacinių sistemų tvarkymo veiklos išdalinimas, bet jos konsolidacija turėtų būti valstybės prioritetas, nes tai leistų sutelkti žinias, kompetenciją, kvalifikaciją ir išteklius vienose rankose ir užtikrinti tinkamą Lietuvos nacionalinių interesų apsaugą bei saugų ir tvarų skaitmeninės infrastruktūros valdymą. Šalia centrinio valstybės informacinių sistemų tvarkytojo stiprinimo, ne mažiau dėmesio turėtų būti skiriama ir atitinkamų priežiūros (kontrolės) institucijų gebėjimų, kompetencijos ir resursų didinimui, kad jos ne tik reaguotų į iškilusias situacijas reaktyviai (dažnu atveju tam pakankamų resursų jos neturi), bet ir gebėtų proaktyviai periodiškai tikrinti ir audituoti ypatingos svarbos ir svarbių informacinių išteklių tvarkytojus, siekiant mažinti galimų incidentų pasikartojimo riziką ateityje.

IV. Siūlomi pokyčiai

Atsižvelgdama į aukščiau išdėstytus argumentus, LVK siūlo imtis šių konkrečių priemonių.

IV.1. Sandorių patikros reikalavimų išplėtimas

Inicijuoti Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo pakeitimą, kuriuo **sandorių atitikties nacionalinio saugumo interesams patikros reikalavimai būtų taikomi visoms institucijoms**, kurios valdo, tvarko ar prižiūri valstybines informacines sistemas, registrus ar kadastrus, kuriuose tvarkomi ypatingos svarbos arba svarbūs valstybės informaciniai ištekliai.

Šis pakeitimas turėtų numatyti, kad kiekviena trečioji šalis, kuriai planuojama suteikti prieigą prie minėtų sistemų ar jų infrastruktūros, privalo būti patikrinta Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos – analogiškai tam, kaip tai taikoma VĮ „Registrų centras“ sandorių šalims.

IV.2. Valstybės informacinių sistemų tvarkymo veiklos konsolidacija ir tvarus finansavimas

LVK visų pirma atkreipia dėmesį į tai, kad valstybės informacinių sistemų, kuriose tvarkomi ypatingos svarbos arba svarbūs valstybės informaciniai ištekliai, **tvarkytojų sąrašas turėtų būti konsoliduojamas siekiant sutelkti gebėjimus, kompetencijas, kvalifikaciją ir resursus patikimose ir periodiškai prižiūrimose ir kontroliuojamuose subjektuose**.

Valstybė turi ne tik reaktyviai reaguoti į incidentus, bet ir proaktyviai imtis priemonių bei skirti pakankamą, nuolatinį finansavimą valstybės informacinių išteklių saugumui. Kibernetinis saugumas nėra būsena, kurią pasiekus galima nustoti investuoti – tai nenutrūkstamas procesas, reikalaujantis nuolatinio dėmesio, kompetencijų, kontrolės, auditų, testavimo ir pakankamų finansinių bei technologinių išteklių, todėl siūlome:

- peržiūrėti ir reikšmingai padidinti valstybės informacinių sistemų, registrų ir kadastrų, įskaitant „e.sveikata“, kibernetiniam saugumui užtikrinti skirtą finansavimą, kad jis atitiktų realų grėsmių lygį ir Europos Sąjungos standartų reikalavimus;
- pereiti nuo reaktyvaus reagavimo prie proaktyvaus kibernetinio saugumo ir skaitmeninio atsparumo valdymo modelio, apimančio nuolatinį valstybės informacinių sistemų atnaujinimą, pažeidžiamumų valdymą, reguliarų testavimą, veiklos tęstinumo užtikrinimą;

+370 5 212 1111
info@lvk.lt
Gedimino pr. 2/1-28
LT-01103 Vilnius
lvk.lt

- įtvirtinti periodinę kompetentingų institucijų vykdomą valstybės informacinių sistemų, registrų ar kadastrų, kuriuose tvarkomi ypatingos svarbos arba svarbūs valstybės informaciniai ištekliai, kontrolę siekiant užtikrinti atitiktį taikomiems BDAR ir Kibernetinio saugumo įstatymo reikalavimams, taip pat aiškiai ir reguliariai viešinti atitinkamų sistemų, registrų ir kadastrų priežiūros bei kontrolės planus ir terminus, kurių laikymasis užtikrintų aukščiausius duomenų apsaugos ir kibernetinio saugumo standartus;
- užtikrinti skaidrų ir reguliarų dialogą su verslo bendruomene dėl valstybės informacinių išteklių saugumo būklės, nes verslo veikla tiesiogiai priklauso nuo šių sistemų patikimumo, duomenų vientisumo ir prieinamumo.

Valstybės registruose, kadastruose ir informacinėse sistemose tvarkomi duomenys yra ne tik valstybės, bet ir kiekvieno verslo subjekto bei kiekvieno piliečio turtas. Jų saugumas – tai pasitikėjimo valstybe, verslo aplinkos stabilumo ir visos visuomenės saugumo klausimas. Sveikatos duomenų atveju tai tampa dar jautresne tema – šių duomenų kompromitavimas pažeistų ne tik asmens privatumą, bet galėtų turėti tiesioginių pasekmių žmogaus sveikatai, gydymo prieinamumui ir sveikatos priežiūros sistemos funkcionalumui.

LVK ragina kompetentingus sprendimų priėmėjus šiuos argumentus įvertinti ir imtis konkrečių, ilgalaikių ir teisiškai pagrįstų priemonių – ne vien reaktyvių atsakomųjų veiksmų – ypatingos svarbos ir svarbių valstybės informacinių išteklių apsaugai sustiprinti.

Esame pasirengę dalyvauti diskusijose ir kurti pokytį kartu.

Pagarbiai

Generalinė direktorė Ineta Rizgelė

Originalas siunčiamas nebus. Akvilė Razumienė, el. p. akvile@lvk.lt, mob. +37060151897.