

**DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SVARBOS VERTINIMO TVARKOS APRAŠO PATVIRTINIMO“ IR LIETUVOS RESPUBLIKOS EKONOMIKOS IR INOVACIJŲ MINISTRO ĮSAKymo „DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ SVARBOS VERTINIMO METODIKOS PATVIRTINIMO“ PROJEKTŲ**

Lietuvos skaitmeninių technologijų sektoriaus asociacija „INFOBALT“ (toliau – Asociacija) išnagrinėjo pakartotinai derinimui pateiktą Lietuvos Respublikos Vyriausybės nutarimo „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“ projektą (toliau – Nutarimo projektas) ir Lietuvos Respublikos ekonomikos ir inovacijų ministro įsakymo „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“ projektą (toliau – Metodikos projektas) (toliau kartu – Projektai), ir teikia savo pastabas.

Leiskite atkreipti dėmesį į tai, kad šiuo raštu mes pateikiame bendresnio ir konceptualesnio pobūdžio pastabas dėl Projektų, ir neteikiame pastabų dėl konkrečių Projekto dokumentų formuluočių. Mūsų vertinimu, pati Metodikos projekto koncepcija reikalauja esminės peržiūros, todėl šiuo metu konkrečių punktų taisymas ar koregavimas nėra prasmingas.

Visų pirma, norime atkreipti dėmesį į tai, kad pagal šiuo metu galiojančio Valstybės informacinių išteklių valdymo įstatymo (toliau - **VIVĮ**) 43<sup>3</sup> straipsnio 2 punktą, Vyriausybės nutarimu turi būti patvirtintas valstybės informacinių išteklių, kurie turi būti prieinami karo, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais, sąrašas. Turint omenyje tai, kad Metodikos tikslas yra surūšiuoti valstybės informacinius išteklius (VII) pagal svarbą ir identifikuoti VII, kurių saugojimas pagal VIVĮ 48 straipsnį būtų privalomas valstybiniuose duomenų centruose (toliau - **VDC**), mes manome, kad sąrašas, patvirtintas pagal VIVĮ 43<sup>3</sup> straipsnio 2 punktą, ir Metodikos, kuri būtų rengiama vadovaujantis VIVĮ 8 straipsniu, poveikio vertinimo sritys turėtų koreliuoti. Visgi, Metodikos poveikio vertinimo sritys nėra susijusios su VIVĮ 43<sup>3</sup> straipsnio 2 punkto logika.

Antra, Metodikoje (Metodikos II skyrius, Priedas Nr. 1) dalis poveikio vertinimo sričių dimensijų ir kriterijų pagal prigimtį turėtų būti taikomi įslaptintos arba riboto naudojimo

informacijos tvarkymui, o ne apskritai visų VII atžvilgiu, pvz., „gynyba, nacionalinis saugumas ir žvalgyba“, „viešasis saugumas ir teisėsauga“. Daug abejonių kelia poveikio srities dimensija „kibernetinis saugumas“. Atitinkamo VII svarbos nustatymo padarinys turėtų būti atitinkamo lygio kibernetinio saugumo priemonių taikymas. Savaimė suprantama, kad kibernetinio saugumo dimensija pati savaimė tiesiogiai negali būti laikoma poveikio srities dimensija. Kibernetinis atsparumas ir informacinis saugumas yra holistinė reikalavimų sistema, taikoma visiems į kibernetinio saugumo teisinių reikalavimų apimtį patekantiems subjektams bei jų valdomoms informacinėms sistemoms.

Šiuo požiūriu Metodika yra ydinga bent **dviem požiūriais**. Visų pirma, duomenys savaimė negali turėti poveikio kibernetiniam saugumui, nors duomenų pobūdis gali lemti informacinės sistemos pobūdį ir svarbą, o tai savo ruožtu gali lemti taikytinų kibernetinio saugumo priemonių ir saugumo kontrolių visumą. Be to, šiuolaikinės informacinės sistemos, jų sauga, atsparumas bei saugumas vertinami ne **pagal fizinę duomenų lokaciją** ar duomenų centro priklausomybę (Žr. VIVĮ 49 straipsnis), bet pagal aukščiau minėtus poveikio ir rizikos nustatymo, rizikos valdymo bei saugumo priemonių parinkimo principus. Kalbant apie kibernetinio saugumo užtikrinimą, NIS2<sup>1</sup> reikalauja, kad kibernetinio saugumo rizikos valdymo priemonėse būtų atsižvelgiama į subjekto priklausomybę nuo tinklų ir informacinių sistemų ir jos turėtų apimti priemones, skirtas incidentų rizikai nustatyti, incidentų prevencijos, atskleidimo, nustatymo, reagavimo į juos bei veiklos atstatymo po jų ir jų poveikio švelninimo priemones. Tinklų ir informacinių sistemų saugumas turėtų apimti saugomų, perduodamų ir tvarkomų duomenų saugumą. Kibernetinio saugumo rizikos valdymo priemonėse turėtų būti numatyta sisteminė analizė, atsižvelgiant į žmogiškąjį veiksnį, kad būtų galima susidaryti visapusišką tinklų ir informacinės sistemos saugumo vaizdą. Be to, kibernetinio saugumo rizikos valdymo priemonėmis turėtų būti sprendžiamas tinklų ir informacinių sistemų fizinis ir aplinkos saugumas, įtraukiant priemones, skirtas sistemoms apsaugoti nuo sistemos gedimų, žmogaus klaidų, piktavališkų veiksmų ar gamtos reiškinių laikantis Europos ir tarptautinių standartų, pvz., įtrauktų į ISO/IEC 27000 seriją<sup>2</sup>.

Kalbant apie antrąjį aspektą, kurio netenkina Metodika, reikia pabrėžti VII kritiškumo įvertinimą valstybės funkcijų, paslaugų ir **veiklos tęstinumo užtikrinimo**,

---

<sup>1</sup> NIS2, 78 preambulės punktas.

<sup>2</sup> NIS2, 79 preambulės punktas.

**atstatymo bei krizės ir incidentų valdymo apsektais.** Esminė Metodikos ir joje numatyto VII vertinimo paskirtis turėtų būtų ne siauras ir labai ribotas bei kartu neapibrėžtas VII surūšiavimas pagal VII esančių duomenų prieinamumo, vientisumo ir konfidencialumo pažeidimo poveikį valstybei, institucijoms ir gyventojams, pagal kurį būtų nustatoma, kokios priklausomybės ar nuosavybės formos duomenų centruose bus talpinami atitinkamo VII duomenys, o VII klasifikacija pagal kritiškumą, poveikį ir rizikingumą tiek valstybės funkcijų, paslaugų ir veiklos tęstinumo užtikrinimui, tiek ir kibernetiniam VII atsparumui. Atitinkamai, Metodikos uždavinys turėtų būti suformuluotas kaip VII klasifikacija pagal kritiškumą įvertinant atskirų VII poveikį kritiškai svarbių valstybės funkcijų, paslaugų ir veiklos atstatymui incidentų ir krizės atvejais, bei valstybės funkcijų, **paslaugų ir veiklos tęstinumo užtikrinimui.** Kaip minėta, kibernetinio saugumo reikalavimai ir iš jų išplaukiančios saugos bei patikimumo užtikrinimo priemonės yra būtent VII svarbos (kritiškumo) nustatymo bei poveikio valstybės funkcijų, paslaugų ir veiklos teikimui įvertinimo padarinys, pasekmė, sudėtinė ir būtina veiklos tęstinumo užtikrinimo proceso dalis. Atitinkamai, atitinkamo kritiškumo VII būtų privalomai taikomi atitinkamo lygio kibernetinio saugumo bei veiklos tęstinumo užtikrinimo reikalavimai. Veiklos tęstinumo valdymui taikomas ISO 22313:2012 standartas, 22317 standartas, krizių valdymui – ISO 22361 standartas, rizikos valdymui – ISO 31000 standartų šeima. Manome, kad Metodika privalo remtis būtent šiomis geriausiomis praktikomis ir metodikomis, kurios yra parengtos pasaulinio lygio ekspertų, ir apibendrintos kompetentingų standartizavimo institucijų.

Trečia, tikėtina, kad įstaigos (VII valdytojai) savo valdomų VII svarbą vertins pagal savo institucijos vidaus veiklos svarbą ir poveikį jai, o ne pagal VII svarbą. Valstybės institucijos veiklos svarba gali būti visai nesusijusi su VII verte ir prieinamumu. Manytina, kad būtent kontroliuojanti institucija, turėdama VII žemėlapi, vertindama VII sąsajas ir kitus kriterijus, turėdama holistinį, vientisą matymą į VII tikrąją vertę valstybės ir viešųjų paslaugų funkcionavimui krizių atveju, turėtų pakankamai geras galimybes atlikti visų VII įvertinimą pagal VII valdytojų pateiktą informaciją.

Mūsų esminis siūlymas būtų konceptualiai pakeisti Metodikos išeitinę poziciją, VII vertinimo uždavinius, tikslą ir būdus. Pagal dabartinį VIVĮ reguliavimą (8 straipsnis), Metodikos tikslas ir poveikis yra itin ribotas, formalus ir siauras. Pagal dabar galiojančią teisinį reguliavimą, Metodikos pagalba bus sukurta ženkliai administracinė našta vien tam, kad būtų

atsakyta į klausimą, kokiame duomenų centre turi būti saugomas vienas ar kitas VII pagal VIVĮ 48, 49 straipsnius.

Matydami pateiktą derinti VIVĮ naują redakciją, matome, jog rengėjams ir toliau stinga bendro holistinio požiūrio. VIVĮ pakeitimais siekiama padaryti kosmetinius pakeitimus ir įtvirtinti atsakomybių fragmentavimą tarp VII valdymo ir kibernetinės saugos reglamentavimo. Atsižvelgiant į tai, mūsų siūlymas būtų ne toliau beprasmiškai koreguoti ir kosmetiškai lipdyti istoriškai susiklosčiusį fragmentuotą teisinį reguliavimą, bet sukonsoliduoti pajėgas į holistinės, vientisos ir nuoseklios skaitmeninės politikos koncepcijos sukūrimą, išnagrinėjant ir permąstant reglamentavimo poreikį, apimtį ir galimą konsolidavimą. Tai leistų strategiškai geriau ir tvariau pasiekti nacionalinius Lietuvos skaitmeninės darbotvarkės tikslus, o kita vertus, tai taip pat atitiktų ir Skaitmeninės Europos programos bei NIS2 direktyvos įgyvendinimo tikslus.

Mielai dalyvautume tokioje darbo grupėje ir visomis išgalėmis prisidėtume prie tvarios, darnios, skaidrios ir efektyvios kibernetinio saugumo bei informacinių technologijų ūkio valdysenos sutvėrimo Lietuvoje!

L. e. p. direktorius

Virgilijus Dirma

[pasirašyta el. parašu]