**VALSTYBĖS ĮMONĖ REGISTRŲ CENTRAS**
Lvivo g. 25-101, 09320 Vilnius, tel. (8 5) 268 8262, el. p. info@registrucentras.lt
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 124110246

Lietuvos Respublikos ekonomikos ir inovacijų ministerijai
Siunčiama per E. pristatymo informacinę sistemą

**DĖL TEISĖS AKTŲ PROJEKTŲ**

Susipažinę su Lietuvos Respublikos Seimo kanceliarijos Teisės aktų informacinėje sistemoje (toliau – TAIS) pakartotinai paskelbtais Lietuvos Respublikos Vyriausybės nutarimo „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo" projektu (TAIS reg. Nr. 22-17258(2), (toliau – Nutarimo projektas) ir Lietuvos Respublikos ekonomikos ir inovacijų ministro įsakymo „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo" projektu (TAIS reg. Nr. 22-17261(2), vadovaudamiesi Lietuvos Respublikos teisėkūros pagrindų įstatymo 9 straipsnio 5 dalimi, nustatančia, kad visi asmenys turi teisę teikti pasiūlymus dėl TAIS paskelbto teisės akto projekto, savo iniciatyva teikiame pastabas ir pasiūlymus dėl Nutarimo projekto.

Nutarimo projektu tvirtinamo Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo projekto 12 punkte nustatyta, kad „VII svarbos vertinimą atliekant šio Aprašo 7.2–7.5 papunkčiuose numatytais atvejais, už VII svarbos vertinimą atsakingais gali būti skiriami informacinės sistemos duomenų valdymo įgaliotinis, **saugos įgaliotinis ir (ar) duomenų apsaugos pareigūnas** (toliau kartu – už VII svarbos vertinimą atsakingi asmenys). VII svarbos vertinimo proceso koordinatoriumi gali būti skiriamas vienas iš šių asmenų."

Atkreipiame dėmesį į tai, kad 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 derinimo pažymoje pateikti argumentai, kad pagal Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 44 straipsnio 2 punktą, saugos įgaliotinis ir duomenų valdymo įgaliotinis gali būti tas pats asmuo savaime nereiškia, kad saugos įgaliotiniui gali būti priskirtos šiai pareigybei nebūdingos funkcijos. Registrų centras 2023 m. sausio 4 d. rašte Nr. S-97 (1.4 E) „Dėl teisės aktų projektų", kai Nutarimo projekte svarbos įvertinimo atsakomybė dar nebuvo priskirta saugos įgaliotiniui, iš anksto akcentavo, kad informacijos svarbos vertinimo funkcijos priskyrimas saugos įgaliotiniui arba administratoriui neatitiktų gerųjų IT valdymo praktikų ir pateikė su tuo susijusius argumentus.

Siekiant, kad informacijos svarbos vertinimas atitiktų tarptautinius saugos standartus, gerąsias IT valdymo praktikas, visuotinai pripažintų organizacijų rekomendacijas, papildomai pažymime, saugos įgaliotinio funkcija yra susijusi su saugos politikos įgyvendinimo priežiūra, pavedimų davimu VII tvarkytojo ar valdytojo darbuotojams[1], bet ne pačiu saugos politikos įgyvendinimu praktikoje. Vadovaujantis LST/ISO IEC 27002[2] standartu, kuris privalomas I kategorijos VII valdytojams ir rekomenduojamas žemesnės svarbos VII valdytojams užtikrinant saugą, už **informacijos svarbos įvertinimą yra atsakingi duomenų savininkai**. Vadovaujantis Valstybės informacinių išteklių valdymo įstatymo 14 straipsnio 2 dalimi, informacinių technologijų auditą atlieka

[1] Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo", 4.7 ir 22.4 papunkčiai ir 24 punktas.
[2] LST/ISO IEC 27002 8.2.1 „Information Classification". Owners of information assets should be accountable for their classification.

visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai. Visuotinai pripažintos tarptautinės Informacinių sistemų valdymo ir audito asociacijos ISACA sertifikuotų informacinių sistemų auditorių (angl. *Certified Information Systems Auditor*) rengimo medžiagoje[3], ISACA sertifikuotų informacijos saugos vadovų (angl. *Certified Information Security Manager*) rengimo medžiagoje[4], Tarptautinio informacinių sistemų saugumo sertifikavimo konsorciumo (ISC) 2 sertifikuotų informacinių sistemų saugumo profesionalų (CISSP) rengimo medžiagoje[5] nurodyta, kad būtent duomenų savininkai yra atsakingi už duomenų klasifikavimą ir nustato duomenų svarbą. COBIT 5 metodikoje[6] taip pat nustatyta, kad duomenų ir (arba) sistemų savininkai priima sprendimus dėl duomenų ir sistemų klasifikavimo ir apsaugos, remiantis numatytu klasifikavimu.

Atsižvelgdami į tai, kas išdėstyta, manome, kad informacijos svarbos vertinimo funkcijos priskyrimas saugos įgaliotiniui akivaizdžiai neatitinka tarptautinių saugos standartų, geruų IT valdymo praktikų ir visuotinai pripažintų organizacijų rekomendacijų, todėl siūlome Nutarimo projektu tvirtinamo Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo projekto 12 punkte nustatyti, kad už VII svarbos vertinimą atsakingais gali būti skiriamas informacinės sistemos duomenų valdymo įgaliotinis ar kitas asmuo, kuriam institucijoje priskirtos duomenų savininko funkcijos.

Edvard Podnebesov, tel. (8 5) 2313600, el. p. Edvard.Podnebesov@registrucentras.lt

[3] „CISA Review Manual" 5.2.3 Inventory and Classification of Information Assets. **Information owner is responsible for the information and should decide on the appropriate classification**, based on organization's data classification and handling policy".

[4] „CISM Review Manual" 1.8. Information Security Strategy Objectives. **The data owner is typically the best source of for determining the potential consequences of „data leakage" and normally the individual determining of the classification level for data**." Data owner – the individual, normally a manager or director, who has responsibility for the integrity, accurate reporting and the use of computerized data.

[5] CISSP Official Study Guide. *Defining Data Classifications*. A data classification identifies the value of the data organization and is critical to protect data confidentiality and integrity. The policy identifies classification labels used within the organization. **It also identifies how data owners can determine proper classification and how personnel should protect data based on classification**.

[6] COBIT 5 Process Assessment Model (PAM): Using COBIT® 5), procesas Nr. AP0 01-BP6AP0 01-BP6 „Define information (data) and system ownership". Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that **owners make decisions about classifying information and systems** and protecting them in line with this classification. COBIT 5 metodika vadovaujasi Lietuvos Respublikos valstybės kontrolė, atlikdama valstybės informacinių išteklių valdymo valstybinius auditus.