UAB „Investicijų ir verslo garantijos“

UAB „Adwisery“ .
Konstitucijos pr. 7, 09308 Vilnius

APIE SĖKMINGAI ĮVYKDYTĄ SUTARTĮ (PROJEKTĄ)

2022 m. spalio 26 d.

UAB „Investicijų ir verslo garantijos“ (toliau – INVEGA), įmonės kodas 110084026, patvirtina, kad UAB „Adwisery“, įmonės kodas 302524912, sėkmingai įgyvendino 2022 m. liepos 21 d. sudarytą Paslaugų teikimo sutartį Nr. r. 4.26.4-65. Įgyvendinimo laikotarpis: nuo 2022 m. liepos 21 d. iki 2022 m. spalio 18 d.

Projekto pavadinimas	**Įgyvendintos projekto veiklos (suteiktos paslaugos)**	**Vertė, Eur be PVM**	**Vertė, Eur su PVM**
Technologinio pažeidžiamumo, asmens duomenų apsaugos ir informacijos, informacinių sistemų informacijos saugumo rizikos ir informacijos saugumo valdymo sistemos trūkumų vertinimo paslaugos	Sutarties (projekto) įgyvendinimo metu suteiktos INVEGA Technologinio pažeidžiamumo, asmens duomenų apsaugos ir informacijos saugos atitikties, informacinių sistemų informacijos saugumo rizikos ir informacijos saugumo valdymo sistemos trūkumų vertinimo paslaugos, kurios apėmė: 1. IT įrenginių technologinio pažeidžiamumo vertinimą; 2. INVEGOS, kaip asmens duomenų valdytojo bei asmens duomenų tvarkymo reikalavimų įgyvendinimo vertinimą; 3. Informacijos saugos priemonių įvertinimą, naudojant šiuos metodus (neapsiribojant išvardintais): interviu, dokumentų analizę, fizinę apžiūrą, išorinių informacinių sistemų pažeidžiamumų testavimą; 4. Informacinių sistemų informacijos saugumo rizikos vertinimą; 5. ISVS trūkumų Lietuvos standarto LST ISO/IEC 27001:2017 reikalavimams vertinimą; 6. Kartu buvo vertinami ir šie informaciniai ištekliai, objektai bei priemonės: 6.1. informacinės sistemos; 6.2. informatikos ir ryšio technologijų infrastruktūra; 6.3. popierinė ir elektroninė informacija, įskaitant asmens duomenis; 6.4. žmogiškieji ištekliai; 6.5. patalpos; 6.6. iš trečiųjų šalių perkamos paslaugos; 6.7. valdomos ir tvarkomos vidaus administravimo informacinės sistemos bei kita programinė įranga; 6.8. kompiuterių tinklas; 6.9. kompiuterinės darbo vietos; 6.10. kita techninė ir programinė įranga, siekiant įvertinti Perkančiosios organizacijos informacijos ir asmens duomenų saugumą, konfidencialumą, vientisumą, prieinamumą. 1.Technologinio pažeidžiamumo vertinimas apėmė:	**10.874,50**	**13.158,15**

	1.1. išorinį informacinių sistemų saugumo vertinimą (patikrinimas atliekamas imituojant potencialaus įsilaužėlio iš interneto veiksmus (angl. Black Box Penetration Testing)), kuris apėmė: 1.1.1. IS išorinio tinklo perimetro patikrinimą; 1.1.2. perimetro tinklo mazgų, pasiekiamų iš interneto, nustatymą; 1.1.3. perimetro tinklo mazguose veikiančių servisų nustatymą ir žinomų pažeidžiamumų patikrinimą bei konfigūracijos analizę (papildomos informacijos apie sistemas surinkimą per klaidų, sisteminius pranešimus, servisų programinę realizaciją); 1.1.4. saityno paslaugų (angl. web service) taikomųjų programų ir saityno paslaugų (angl. web service) saugumo vertinimą; 1.1.5. duomenų teikimui naudojamų technologijų saugumo vertinimą; 1.1.6. nustačius pažeidžiamumus, atliktas įsilaužimo testas; 1.1.7. aptikus iš interneto pasiekiamų paslaugų (angl. service), reikalaujančių naudotojo autentikavimo, atliktas išorinės paslaugos slaptažodžių auditas. Tikrinanta, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti, ar saugos sistemos pastebi tokius bandymus ir informuoja administratorius, ar imamasi tinkamų reagavimo veiksmų. 1.2. vidinį informacinių sistemų saugumo vertinimą (patikrinimas atliekamas turint naudotojo prisijungimo duomenis (angl. White Box Penetration Testing)), kuris apėmė: 1.2.1. IS duomenų bazių valdymo sistemos saugumo vertinimą; 1.2.2. duomenų perdavimo tinklo įrenginių saugumo vertinimą; 1.2.3. elektroninio pašto apsaugos sistemos efektyvumo vertinimą; 1.2.4. tarnybinių stočių saugumo vertinimą; 1.2.5. iki 10 kompiuterizuotos darbo vietų patikrinimą. 1.3. Atlikus Technologinio pažeidžiamumo vertinimą parengta ir pateikta Technologinio pažeidžiamumo vertinimo ataskaita su rekomendacijomis, kaip pašalinti nustatytas saugumo spragas. 2. INVEGA Asmens duomenų apsaugos priemonių vertinimo (toliau – Atitikties vertinimas) paslaugas, o būtent: 2.1.. Klausimyno vertinimui parengimas; 2.2. Informacijos apie turimas priemones surinkimą ir analizę (informacijos surinkimas ir analizė atliekama dokumentinės analizės, interviu ir kitų metodų pagalba), kurias sudaro: 2.2.1. Tinklo ir techniniai ištekliai; 2.2.2. Procesai ir procedūras, susijusios su asmens duomenų tvarkymu; 2.2.3. Duomenų tvarkymo dalyviai; 2.2.4. Veiklos sritys ir duomenų tvarkymo mąstai; 2.2.5. Priemonių atitikties įvertinimas ir pagrindimas; 2.2.6. Asmens duomenų tvarkymo taisyklių peržiūra; 2.2.7. Duomenų veiklos įrašų peržiūra; 2.2.8. Asmens duomenų pareigūnui priskirtų funkcijų įgyvendinimo vertinimas; 2.2.9. Atitikties vertinimui pagrįsti įrodymų surinkimas; 2.2.10. Nustatytoms neatitiktims šalinimo priemonių plano parengimas.		

	2.3. Atlikus Atitikties vertinimą parengta ir pateiktas Atitikties vertinimo ataskaita ir nustatytų neatitikčių šalinimo planas, tinkantys įkelti į ARSIS. 3. INVEGA Informacinių sistemų informacijos saugumo rizikos vertinimo (toliau – Rizikos vertinimas) paslaugos, o būtent: 3.1. įvertinta informacinių išteklių įtaka konfidencialumui, vientisumui ir prieinamumui; 3.2. atliktas grėsmių ir pažeidžiamumų įvertinimas; 3.3. įvertintos grėsmių tikimybės ir jų poveikis (pasekmės); 3.4. nustatytas rizikos lygis; 3.5. nustatytos ir įvertintos esamos rizikos valdymo priemonės; 3.6. įvertintas rizikos priimtinumo lygis ir parinktos rizikos valdymo priemonės; 3.7. nustatytos likutinės rizikos. Atlikus Rizikos vertinimą parengta Rizikos vertinimo ataskaita, įskaitant ir rizikos valdymo priemonių planą. 4. ISVS trūkumų (angl. Gap analysis) Lietuvos standarto LST ISO/IEC 27001:2017 reikalavimams vertinimas (toliau - ISVS trūkumų vertinimas) atliktas vadovaujantis Lietuvos standarto LST ISO/IEC 27001:2017 (toliau – Standartas) reikalavimais ir apėmė: 4.1. Klausimyno vertinimui parengimą; 4.2. Informacijos apie esamą ISVS surinkimą ir analizę (informacijos surinkimas ir analizė turi būti atliekama dokumentinės analizės, interviu ir kitų metodų pagalba); 4.3. ISVS trūkumų įvertinimą ir aprašymą; 4.4. ISVS trūkumų šalinimo priemonių plano parengimą.		

UAB „Investicijų ir verslo garantijos“ technologinio pažeidžiamumo, asmens duomenų apsaugos ir informacijos, informacinių sistemų informacijos saugumo rizikos ir informacijos saugumo valdymo sistemos trūkumų vertinimas atliktas profesionaliai. UAB „Investicijų ir verslo garantijos“ yra patenkinta projekte dalyvavusių ekspertų kompetencija, gebėjimu įsigilinti į organizacijos poreikius ir sutartinių įsipareigojimų įgyvendinimo terminais.

Pasirašė:

IT Skyriaus vadovas
Aleksandras Šilkonis